GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of "Seminars", "Proceedings", "Monographs" and "Dissertation Award", current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English.

Information: http://www.gi-ev.de/LNI

ISSN 1617-5468
ISBN 3-88579-376-8

This volume contains papers from the July 2004 ESF-sponsored workshop on Electronic Voting in Europe – Technology, Law, Politics and Society held in Schloß Hofen/Bregenz at the wonderful lake of Constance in Austria. Topics of the contributions cover all aspects (technology, law, politics and society) of Electronic Voting in the European countries.

Alexander Prosser, Robert Krimmer (Eds.): Electronic Voting in Europe

P-47

GI-Edition

Lecture Notes in Informatics

Alexander Prosser, Robert Krimmer (Eds.)

Electronic Voting in Europe – Technology, Law, Politics and Society

**Workshop of the ESF TED Programme together with GI and OCG
July, 7th–9th, 2004 in Schloß Hofen/Bregenz, Lake of Constance, Austria**

Proceedings

Alexander Prosser, Robert Krimmer (Eds.)

Electronic Voting in Europe
Technology, Law, Politics and Society

Workshop of the ESF TED Programme
together with GI and OCG

July, 7th – 9th, 2004
in Schloß Hofen/Bregenz,
Lake of Constance, Austria

Gesellschaft für Informatik 2004

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-47

ISBN 3-88579-376-8
ISSN 1617-5468

Volume Editors

ao.Prof. Dr. Alexander Prosser
Institute for Information Processing, Information Business and Process Management
Department Production Management
Vienna University of Economics and Business Administration
A-1200 Vienna, AUSTRIA
Email: Alexander.Prosser@wu-wien.ac.at,
Mag. Robert Krimmer
Institute for Information Processing, Information Business and Process Management
Department Production Management
Vienna University of Economics and Business Administration
A-1200 Vienna, AUSTRIA
Email: Robert.Krimmer@wu-wien.ac.at

Series Editorial Board

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

The emergence of the Internet and other electronic-commerce technologies has fundamentally altered the environment in which governments deliver services to citizens, businesses, and other government entities. Many countries have launched electronic government programs to develop a new way of interaction with the government for companies and citizens. Too often those efforts only concentrate on the administrative side neglecting the democratic processes. Still there are ambitious governments and institutions that have taken a step ahead to develop electronic democracy initiatives. Electronic voting, being the most important form of decision making by citizens, is the main driver for such projects and at the same time the biggest obstacle due to the complexity of the topic.

It is therefore important to discuss the concepts and experiences made with electronic voting. One key research program for this is the "Towards Electronic Democracy" project sponsored by the European Science Foundation. The aim of the program is to draw on the modern methods of decision analysis and group decision support, deployed over the WWW, in order to involve the public in decisions.

During the 2003 TED summer school in Varenna the idea came up to organize a specialised workshop to discuss the developments in electronic voting in Europe not only from the perspective of one isolated discipline but in an interdisciplinary approach covering technology, law, politics and society. Together with the conference location in Bregenz at the beautiful Lake of Constance, surrounded by Switzerland, Germany and Austria, it convinced the steering committee to go ahead with the project.

We wish to thank Wolfgang Polasek, Simon French, Fabrizio Ruggeri and the remaining members of the TED steering committee for making this interesting workshop with 20 presentations from 11 European countries possible. It is the largest accumulation of information on electronic voting to date.

Further thanks go to the German Society of Informatics and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Computer Society with its forum Electronic Government that has now hosted the working group E-Democracy/E-Voting for the third year. The working group has been a forum for interesting discussions that would not have been possible otherwise.

We gratefully acknowledge the support of Jürgen Weiss, MP as we could always approach him for advice and support with his long year experience in organizing elections.

Finally, we also want to thank our colleagues from the Vienna University of Economics and Business Administration, Department of Production Management, who have supported us since our initial idea to research on the topic of e-Voting.

Vienna, July 2004 Alexander Prosser, Robert Krimmer

Programme Committee

- Alexander Prosser, Austria (Chairman)
- Nadja Braun, Switzerland
- Wolfgang Polasek, Switzerland
- Robert Müller-Török, Germany
- Jochen Scholl, USA
- Roland Traunmüller, Austria

Organizing Committee

- Robert Krimmer (Chairman)
- Robert Kofler
- Martin Karl Unger

Sponsors

European Science Foundation

Gesellschaft für Informatik

Austrian Computer Society (OCG)

Austrian Chamber of Commerce

Regional Government of Vorarlberg

Preface

by Univ. Prof. Dr. Andreas Khol MP (President of the Austrian National Council)
and Jürgen Weiß MP (President of the Austrian Federal Council)

These times are a period of rapid political and technological change. Old and new political systems – local, regional, national, supranational or global – are in transition. Their underlying conceptions, preconditions and philosophical foundations are questioned and contested. One response of thinkers, politicians and citizens has been to endorse modern communication technologies and regard them as means to renew the practice of politics and the space of the political. Other responses have led to more critical and reflective discourses on democracy and constitutionalism under the conditions of late modernity and its particular relation to technology. They are concerned with the oppositions and antagonisms asserting themselves against democracy be it in the name of national interest, economic or technological necessity. At the same time, they call our attention to the threat of a decline of democratic deliberation and decision-making within the traditional institutions of representative nation states. The response they offer is a reassessment of our concepts of democratic freedom, democratic practice and citizenship.

Seen from this perspective the new communication technologies have a high democratic potential. They offer powerful tools for exchanging information, engaging in discussion, campaigning and creating awareness about political issues. However, experience shows that reliance on technology cannot be the solution for the current problems our political systems face. Particularly lower voter turnout is not – with the exception of a few cases – a result of being difficult to vote by traditional means. It is more likely to be a symptom of dissatisfaction with or even ignorance of politics. Often it is dissatisfaction with the party one voted for previously and the first step to shift one's party affiliation at the next occasion.

Hence, the Austrian Parliament endorses the second response outlined above and uses new communication technologies to participate in the practices of citizenisation and to encourage citizens to take part in the discussion of our common affairs. Conscious of the questions of social and epistemic justice and the difficult and often criticised relation between communication and power, the Austrian Parliament and the Austrian Government aim to widen transparency, openness and inclusiveness of the political process with the help of new technologies. An outstanding example is the "Austrian Convention", a forum of politicians and experts that discusses constitutional reform. A functional and well-designed website provides immediate access to all proceedings. Citizens can get in touch with the conventioneers and the secretariat of the Convention and submit their thoughts and ideas on the Convention and the new constitution. Currently we are working on a new and easily accessible database which will provide not only a lot of background information on the context of the Convention but which will also be a step towards more interaction between the Parliament and civil society.

Yet, there are serious concerns and doubts about e-voting. Can e-voting help to resolve the problems we currently and face? To what changes of the system of representative democracy might it lead in the long run? Therefore we welcome your initiative and your workshop on electronic voting in Europe, which aims to address a lot of crucial issues in an interdisciplinary context. We hope and wish that your discussions will provide insights and impulses for the discourse on law, politics, society and technology.

Vienna, June 2004

Univ. Prof. Dr. Andreas Khol MP
President of the Austrian National Council

Jürgen Weiss MP
President of the Austrian Federal Council

Content

Keynotes

Towards European Standards on Electronic Voting

Michael Remmert

Council of Europe, Strasbourg Department
Avenue de l'Europe
67075 Strasbourg Cedex, FRANCE
Michael.Remmert @coe.int

Abstract: Michael Remmert is project manager of the project "Making democratic institutions work" in the Council of Europe. The Council of Europe has been working since 2002 on a set of European standards on the legal, operational and technical aspects of electronic voting. This keynote gives insights on the progress and the work done so far.

The Council of Europe is a pan-European inter-governmental organisation with 45 member states, covering virtually the entire continent of Europe, thus representing 800 million Europeans. It seeks to develop common democratic and legal principles through standard setting and a culture of co-operation. With regard to new information and communication technologies, the Council of Europe has developed minimum standards in areas that are of concern to all member states, from cybercrime to data protection. It constantly highlights the importance of the human and democratic dimension of communication and promotes e-inclusion and the empowerment of citizens in a democratic information society in such a way as to take advantage of opportunities and prevent risks which may result from the new information and communication technologies.

Against this background, the Council of Europe has set up a committee, which is currently preparing a set of European standards on the legal, operational and technical aspects of electronic voting (e-voting). After some exploratory work in 2002, the first meeting of the Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical aspects of e-voting (IP1-S-EE) was held in February 2003. The Ad Hoc Group has been supported by two subgroups, one dealing with legal and operational aspects of e-voting, the other with technical aspects.

Common standards on e-voting, reflecting and applying the principles of democratic elections and referendums to the specificities of e-voting, are key to guaranteeing the respect of all the principles of democratic elections and referendums when using e-voting, and thus building trust and confidence in domestic e-voting schemes.

The standards on e-voting are being prepared in such a way as to be accepted and applied by governments and industry alike. The Council of Europe is preparing standards at three levels:

Legal standards, reflecting the fundamental principles of elections enshrined in international legal instruments.

Operational standards, regarding basic matters of organisation and procedure with regard to e-elections which ensure the respect of the fundamental legal standards.

Core technical requirements, which are required to deliver operational standards in a secure and cost-effective manner while ensuring interoperability across devices and enabling control at any stage of the election process.

The Ad Hoc Group uses the following definition of the term 'e-voting': "An election or referendum that involves the use of electronic means in at least the casting of the vote". The term 'remote e-voting' refers to "e-voting where the casting of the vote is done by a device not controlled by an election official".

The key assumption adopted by IP1-S-EE is that e-voting should be at least as reliable and secure as democratic elections and referendums which do not involve the use of electronic means, and that it should be in compliance with the fundamental principles of democratic elections and referendums (universal, free, equal, secret and direct elections).

The standards will cover all the elements of an e-enabled election, i.e. the notification of an election, voter registration, candidate nomination, voting, calculation of results and audit.

The reasons for introducing or considering the introduction of e-voting in one or more stages of a political election or referendum can differ from country to country. Depending on the specific domestic context in each country, these reasons include:

- enabling voters to cast their vote from a place other than the polling station in their voting district;
- facilitating the casting of the vote by the voter;
- facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;
- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;
- increasing voter turnout by providing additional voting channels;
- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;
- delivering voting results reliably and more quickly; and
- providing the electorate with a better service in pursuit of democracy, by offering a variety of voting channels.

Despite the above-mentioned potential benefits of the introduction of e-voting, it should be noted that modernising how people vote will not, per se, improve democratic participation. Failure to do so, however, is likely to weaken the credibility and legitimacy of democratic institutions.

As long as e-voting is not universally available, it should not replace the traditional way of casting a paper ballot in a polling station, it should remain an optional and additional channel. It should be considered to provide the electorate with opportunities for multi-channel voting, i.e. a combination of traditional paper ballot, kiosk/poll site e-voting and remote e-voting, in order to maximise bnefits for citizens who have access to, and are confident in using new technologies without penalising those unfamiliar with such systems.

Only e-enabled voting systems which are efficient, secure, technically robust and readily accessible to all voters will build the public trust to such an extent as to make it feasible to hold large-scale e-enabled elections.

In order to ensure the privacy and equality of suffrage, it must be ensured that only persons who are entitled to do so vote at an e-enabled election, no voter casts his/her vote more than once, and each vote validly cast is only counted once when election results are calculated.

The compliance of e-voting systems with secrecy requirements should be ensured according to the following principles:

- Any authentication procedure should be such as to prevent the identity of the voter being disclosed to others;
- Voters should be given access to particular electronic ballot boxes in a number sufficient to protect the identity of any individual voter using the ballot box;
- No ballot should be disclosed in any manner during the administration of the election, or afterwards, that permits the voter who cast the ballot to be identified.

Finally, specific and satisfactory solutions must be put into place in countries where the electoral system allows voters to change a previously cast postal vote on election day (e.g. Sweden), or where a judicial authority is authorised by law under specific circumstances to ascertain by whom, where and by what means any ballot was cast (e.g. United Kingdom).

Once adopted, the Council of Europe standards for e-voting will be applicable to e-enabled voting systems in supervised environments (polling stations, mobile kiosks etc.), but also to remote e-voting (internet, telephone, etc.). The standards could be used by member states as benchmarks for the setting-up of e-voting systems and the evaluation of pilot projects. They should be valid in a long-term perspective and irrespective of changes in technology.

It is expected that the Committee of Ministers of the Council of Europe will be able to adopt a Recommendation to member states on e-voting in the autumn of 2004.

With regard to possible follow-up at the Council of Europe to the Recommendation on e-voting, the following is presently being considered: As e-voting is a new and rapidly developing area of policy and technology, standards and requirements need to keep abreast of, and where possible anticipate new devlopments. In recognition of this, the e-voting Committee is likely to suggest to the Committee of Ministers to recommend to member states to keep their own position on e-voting under review and report back to the Council of Europe the results of any review that they have conducted. It is anticipated that the Council may look again at this issue within the two years following the adoption of the Recommendation and member states may bear this timing in mind when deciding whether, and if so when, a review is appropriate in their particular circumstances. The compliance of e-voting systems with secrecy requirements should be ensured.

E-Democracy in E-Austria

Christian Rupp

Austrian Federal Chancellery
Chief Information Office
Ballhausplatz 2
1014, Vienna, AUSTRIA
Christian.Rupp@cio.gv.at

Abstract: Christian Rupp has been appointed Federal Executive Secretary of E-Government in May of 2003. At that point of time a new E-Government Platform was introduced. He reports on the current developments of E-Democracy in Austria.

A new-networked economy and a knowledge-based information society have emerged in our midst. The way people live, learn, work and relate to each other is being unalterably changed. The digital revolution is leading to the development of entirely new forms of social and economic interaction and new communities in a borderless cyberspace. Free flow of information and ideas has sparked an explosive growth of knowledge and its myriad new applications. As a result, economic and social structures and relations are being transformed.

In the private sector, citizens have become used to using the Internet for business transactions - they expect the same level of service from their government agencies. Hence, e-government has become one of the main concerns in the administration.

With the decision of the Council of Ministers of the Austrian Federal Government in May 2003 an E-Government Platform at political level has been set up in June 2003 which is chaired by the Chancellor in order to demonstrate the high priority of the implementation of E-Government. The platform is composed by the Vice-Chancellor, the Federal Minister of Finance, the Federal Minister of the Interior, the Federal Minister of Justice, the State Secretary in the Federal Chancellery, governors of the federal provinces , the president of the association of Austrian cities and towns, the president of the Austrian association of municipalities, the business sector (Presidents of the Federal Chamber of Commerce, of the Austrian Social Security Institutions and of the National Conference on Liberal Professions), the Federal Chief Information Officer, several external experts and the Federal Executive Secretary for E-Government.

This platform has to agree on an Austrian E-Government Roadmap (nearly 100 projects until 2005) and to ensure the overall coordination of its implementation.

An E-Cooperation Board under the head of the Federal Executive Secretary for E-Government is in charge of the preparation of the Roadmap and the monitoring of the ongoing activities. In this board each ministry, each federal province, experts from the associations of municipalities, cities and towns are represented as well as experts of chamber organisations. A separate business platform involves nearly 150 companies in the E-government field.

This construction of an E-Government Platform an E-Cooperation Board and a business platform guarantees the communication between all stakeholders and political parties as well as representations of interests.

E-Government enables citizens to have access to their government whenever they need it, whether it is after hours or from abroad. This service focus to the citizen is at least as important as cost savings, which are, of course, an essential driver in our e-government strategy as well. The maturity in e-government services, to businesses as well as to individual citizens, will also be an important factor to determine the attractiveness of a city or region within the European Union. It is therefore of particular interest that Austria took fourth place in the 2003 overall e-government ranking within the European Union and came in second in services offered completely online.

E-Democracy systems and also E-Voting require strict identification and authentication of the individual. In Austria the first Citizen Cards are already on the market. The concept of the Citizen's Card (Authentication and Identification – Digital Signature) is being rounded off with the new tool of the digital signature for public administrations. In accordance with the principle of technological neutrality, the electronic signature can also be made via mobile phone. With the application of the mobile phone signature, Austria puts itself in an internationally leading role. This technology enables also sensitive government services, such as E-Voting, to be delivered in a secure manner to identified and authenticated citizens.

In the past, E-Government has focused on access to administrative functions; however, the Internet can also be used to exercise one's democratic rights.

In administrative E-Government services, efforts have now been focusing on the transaction level, whereas in the area of E-Democracy, efforts are typically still on the level of information or communication. It should be noted that E-Democracy services may cover all stages of the political process from agenda setting over deliberation and decision to monitoring of decisions made.

Even though the distinction between deliberative processes ("E-Participation") and decision making ("E-Voting") can be found in the literature, it has to be noted that a voting process can be a part of any of the above stages.

	E-Government	E-Democracy
Information	Download of forms, guides and "who-is-who", law information system, like http://ris.bka.gv.at http://help.gv.at http://www.austria.gv.at http://www.e-government.gv.at	Download of political programmes or facts relevant to a political discussion, pages run by representatives, like http://www.parlinkom.gv.at http://www.konvent.gv.at http://www.oevp.at http://www.spoe.at http://www.gruene.at http://www.fpoe.at
Communication	Electronic Web forms to start an administrative process: http://www.kremsmuenster.at http://www.weikersdorf.at http://www.wien.at http://www.service.steiermark.at	E-mail communication with representatives, moderated discussion fora on specific political topics: http://www.klassezukunft.at http://dafne.twoday.net http://mariegoessmscam.twoday.net http://enzersdorf.twoday.net
Transaction	Tax declarations, registration of abode, e-procurement, public library system, eg.: https://finanzonline.bmf.gv.at http://www.lieferanzeiger.at http://www.zustellung.gv.at	Voting, initiative, petition, eg.: http://www.e-voting.at

Figure 1: E-Government and E-Democracy Austrian best pracitice

The Austrian E-Government roadmap encompasses E-Voting, in a first step for citizens abroad, where the first field trials are expected in 2005, two test elections among students have already taken place.

However, the challenges in deploying viable e-voting solutions are formidable: Some examples of E-Government and E-Democracy in E-Austria:

- @ The protection of privacy and voter anonymity.
- @ The unequivocal identification of the voter.
- @ The implementation of the election committee in its functions to ensure verifiability and reproducibility of the election.
- @ The protection from sabotage either by external attacks or by voters or candidates attempting to disturb the elections.

Even though organisational safeguards are of course important, an E-Voting system has to technically guarantee compliance with these principles. We should be aware that an election is certainly one of the most regulated processes in a modern democracy and that it is also one of the most sensitive because it touches the core of our society.

In a modern democracy we have also the duty to close the gap between the technology-empowered and the technology-excluded communities on our planet as well as to the lack of information transfers in and between these communities. The developing world and transition economies comprise the largest portion of the digital and knowledge divides.

This workshop “Electronic Voting in Europe” will provide an overview of current E-Voting activities in Europe, their legal and technical approach and will report experience from various field trials. May it help a better understanding of the issues in electronic voting and pave the way for reliable and secure e-democracy systems in the future.

The Dimensions of Electronic Voting
Technology, Law, Politics and Society

Alexander Prosser, Robert Krimmer

Institute for Information Processing, Information Business and Process Management
Department Production Management Institution
Vienna University of Economics and Business Administration
Pappenheimgasse 35/5
A-1200 Vienna, AUSTRIA
{Alexander.Prosser | Robert.Krimmer}@wu-wien.ac.at

Abstract: Since the Internet boom in the 1990's the question has arisen, will it be possible to vote via the Internet one day. In many European countries and around the world initiatives of research institutions, private organisations and governments have tried to provide an electronic solution to this key democratic process.
As many projects there are, as many different strategies lie behind that. Based on similar studies out of the United Kingdom, Germany, the Netherlands and Switzerland, this article develops a register of criteria to assess and compare different E-Voting initiatives on national and project level using four key dimensions: Technology, Law, Politics and Society.

1 Introduction

Since the beginning of the big Internet boom in the 1990's a lot has been discussed how to use information technology in public administration. Still it became clear in a very early stage that experiences made in the E-Business field cannot be attributed to public administration in the same manner. In this way the term "electronic government" evolved as a new name for the field of public information systems. In Europe the electronic government movement is hyped and by politicians it is often mistaken solely for the IT-enabled support of administrative tasks in the government[1]. This leaves out a complete field of interaction between the citizens and government – the area of democratic processes, especially elections.

[1] For the opinion of MP's of the Austrian Federal National council see the explorative study in [AsFr04]

Therefore definitions of the term electronic government include these processes as well. Scholl for example defines in [Scho03] electronic government as, "the use of information technology to support government operations, engage citizens, and provide government services" which includes not only electronic administration but also electronic participation by citizens. This differentiation can also be found in Europe where Reinemann and von Lucke [LuRe04] distinguish E-Workflows and E-Democracy. Furthermore von Lucke and Reinemann define E-Democracy as the electronic representation of the democratic processes, which Parycek and Seeboeck devide in three subprocesses [PaSe03], (i) Information acquisition, (ii) Formation of an opinion and (iii) The decision itself. Electronic Democracy hereby contains two aims – the field of E-Participation (decision preparation, therefore consisting of process (i) and (ii)) and the field of E-Voting (decision making, therefore process (iii)).

For applications in the Internet one can distinguish them by their level of technical complexity. Combining the technical complexity with the political processes one can develop an E-Democracy application framework. This framework follows an approach introduced by the EU Forum E-Democracy working group [MacA03] where they match the political processes with the technical complexity.

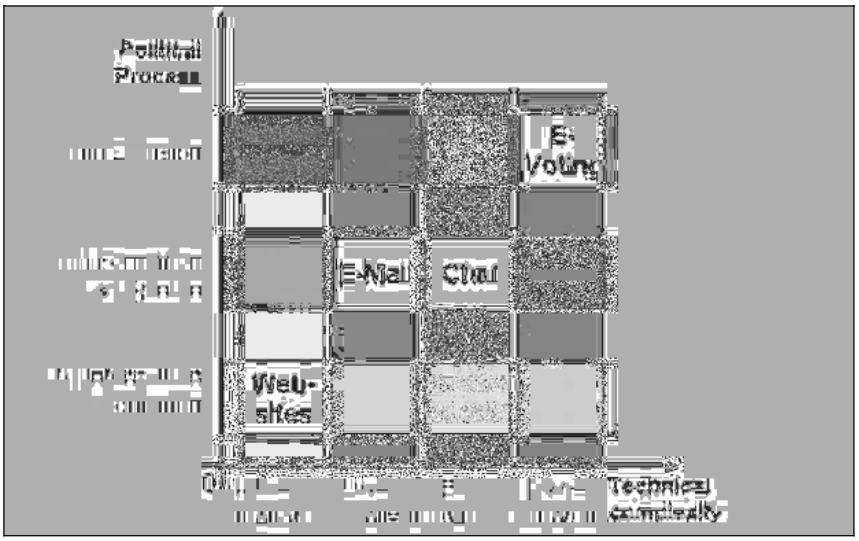


Figure 1: E-Democracy Application Framework

This results in four application types that are depicted in figure 1: (i) Websites as information provision for citizens, (ii) E-Mail communication with politicians as uni-directional as communication is asynchronous, (iii) Chats with politicians as discussion takes place at the same time, and finally (iv) E-Voting where a decision is ultimately made.

Especially IT-enabling the core process of a democracy, the voting itself, leads to different imaginations where the future society could end up. In 2001, Aström [Astr01] depicted the following three possibilities:

1.) Thin Democracy: The voter is electing her representative and is constantly informed by the representative.
2.) Strong Democracy: In this model the citizen is constantly deciding on options presented by the politicians; there is always interaction between citizen and politician.
3.) Quick Democracy: In a quick democracy, the politician is only a handyman for the citizen, as the voter decides on any decision herself.

Those scenarios often come into discussion when talking about electronic voting but often cover up the real issues when talking about E-Voting like i.e. security, public acceptance of new technologies and so on. Also voting is a process with a lot of tradition involved – people have fought in some countries for this right for years and therefore discussions about this topic have to be led with care. Hence conclusions cannot be easily drawn or experiences transformed from one country to the other. This paper therefore tries to give a systematic overview of factors involved in a discussion on electronic voting, so E-Voting initiatives become comparable beyond country borders.

2 Existing Cross-National Research

In the field of public IT offerings comparing initiatives helps improving the applications. In electronic government the European Union is leading the way by organizing a yearly benchmark. Here the assigned company, Cap Gemini, is conducting a survey and counts and matches the number of administrative services to citizens and to businesses offered by each country [CG04].

For electronic democracy applications such benchmarks do not exist, nor is plenty of research available.

The first trial to describe different approaches to implement E-Voting was done in 2003 by Braun, Prosser and Krimmer where they compared the Swiss and Austrian initiatives in [BPK03]. Therein they identified three areas to include in their research: technology, law and socio-politics.

A similar approach was followed by Kersting in [Kers04] where he compared the E-Voting initiatives in Austria, Germany and Switzerland descriptively. He also looked at legal settings, technological solutions and the political necessity for introducing new forms of decision making.

Another paper on the scarce field of crossnational research was the report of the EU Forum led by Ann Macintosh from the Center for Teledemocracy at Napier University in the United Kingdom [MacA03]. Her working group tried to compare E-Democracy projects across European borders. It was structured in twelve points which concentrated on policy questions as depicted in table 1:

1	Stage in decision making
2	Level of engagement
3	Actors
4	Resources
5	Technologies
6	Rules of engagement
7	Duration & sustainability
8	Scale
9	Accessibility
10	Promotion
11	Evaluation
12	Outcomes Critical factors for success

Table 1: EU Forum Case study template

On the project and application level, Moosmann and Baumberger from the institute for business and administration from the University of applied sciences in Bern, did a study on electronic voting application design and security [MoBa03] and focused on manipulations and Denial of Service attacks.

Leenes and Svensson from the University of Twente In the Netherlands conducted an European wide study on E-Voting approaches where they distinguished in two levels – national and project based experiences [LeSv02; LeSv03].

Integrating and extending these several papers was the basis for the model that is presented in the following chapter. It allows comparing E-Voting initiatives across country borders.

3 The Model

In the previous chapter we presented several studies which all had the aim to compare different E-Voting approaches. All papers had in common not to concentrate on a single field of knowledge but to integrate different sciences like technology or law. But especially in the field of electronic democracy it is not only technological or legal questions determining how the application has to look like, but also politics and society influence E-Voting as proposed by Braun, Prosser and Krimmer in [BPK03]. Therefore one has to first differentiate four separate dimensions: (i) **Politics**, (ii) **Law**, (iii) **Technology**, and (iv) **Society**.

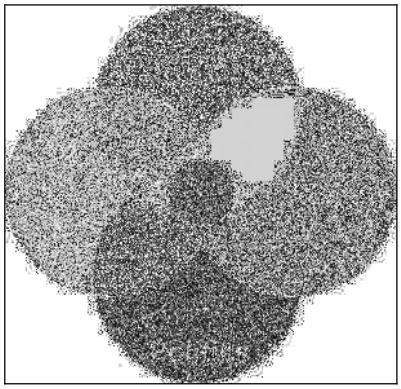


Figure 2: Dimensions of E-Voting

When using the four dimensions one has to distinguish two levels, as used by Leenes and Svensson in [LeSv03]. In their study they used a project and a national level to get clear results. We included this approach in our model as it is clear that electronic democracy applications are prototyped in a small environment and then rolled out on a larger level[2]. This usually leads to an unaccounted bias in country studies, when it is ignored in the benchmark, as pilot experiences are often mistaken for national experiences. By introducing the two levels, a national and a project level, one can rule out such a bias[3].

3.1 Dimensional Factors on the National Level

In the next step we describe the different points attributed to the separate dimensions on the national level. As the political system builds the foundation, we start with **(i) Politics**. In this field it is important to know what kind of *political system* is found (constitutional monarchy, parliamentary democracy, etc.), the *method* and *frequency of elections* as well as general *statistics on elections* (eligible voters, electoral districts, number of polling stations). A second important point for politics is the *official attitude* towards E-Voting. The *stage in the policy making process* is relevant, the *aim of the policy*, and if an *official organisation* is planned for the implementation of E-Voting (maybe even integrated in an E-Government organisation).

The kind of *legal system* is the key element of **(ii) Law**, with the *electoral law* in special as the basis for the technological solution. For E-Voting the existing *legal principles for elections* are important, the way E-Voting is (could be) implemented and in which stage E-Voting is in the *legislation-making process*.

---

[2] For example the German Ministry of the Interior follows a way of implementing E-Democracy applications on a step by step basis as described in [KaRu03].
[3] This also a problem f [CG04].

In the third dimensions **(iii) Technology** it is important to know the status of *registers* in general, in special a register of *citizens* and as a subgroup of that of *eligible voters*. Further important technological infrastructure questions are the *implementation* of a *digital national ID card*, of the *digital signature* and if the adoption of *international E-Voting standards* are planned. Furthermore it is interesting to know the *level of E-Government offerings* in general.

For the last dimension of (iv) **society** the factors concentrate basically to *the level of political participation*, the *turnout for postal voting* and the *public attitude towards new technologies* and *E-Voting* in particular. It is also necessary to know the *penetration rate of telephones*, *mobile phones*, *personal computers*, *the Internet including broadband access*, and finally *Internet transactions* in the society.

Using these four dimensions one can do a basic assessment of approaches towards E-Voting on a National level. As E-Voting has not been implemented on a national level so far, there usually is more than one E-Voting project per country. Therefore the more detailed especially technological points are included in the next part.

3.2 E-Voting Project Level

As pointed out before the national and the project level differ a lot – especially the key dimensions are not applicable in that way to the project level. Out of this reason we differentiate the project description in three parts: (i) **Project overview**, (ii) The **used technology** and (iii) The **outcome of the project**.

For the project overview it is useful to include the *type of project*, *status*, *duration*, *sustainability*, *setting* (public/private), and the *aim* of the project. Further aspects include the available *resources*, consisting of the *budget* and *kind of funding*. For an assessment it is also necessary to know the *actors*, the *initiator* and if there is *scientifically background* to the project. The *scope of the project*, i.e. the *legal validity*, the *participants* and the *turnout* and finally the used *promotion* and *advertisement channels* are important general project determinants.

As the technology is essential for the success of an E-Voting project, the second point is the (ii) used technology. This consists of general information, the E-Voting procedure and security. For the *general information*, this should be on *hard-* and *software used*, the *developer* and the *forms of E-Voting* that were used.

For the *E-Voting procedure* it is important to know the way the *legal principles of elections equal and free* were guarantee, how the voter is *identified*, how the *anonymity* is guaranteed as well as if an *election committee function* is implemented. For the E-Voting security this consists of *certification of the system*, *system stability* and *endurance testing*, *organisational protection*, *crisis management*, *protection from Denial of Service attacks* as well as *virii*, *Trojan horses* or *man-in-the-middle* and *spoofing* attacks. For the voting procedure itself the *double voting* and *proxy voting* is important as well as how acts of *sabotage* can be identified, and if *pre-counting of votes* can be inhibited (i.e. knowing the results before the end of the election). The *rules of engagement* are a final point for the technology side of the projects.

The third and most important point is the (iii) **Outcome of the project**. This is consisting of the *results of an evaluation*, *other outcomes*, *critical success factors* and the *contentedness of the voters*.

Having these points as part of a project description one can give an all-embracing overview one's project experience.

3.3 Assessment

The model consists out of two points of view, a general and a detailed project view. These views are each divided in relevant aspects, on the national level in technology, law, politics and society and on the project level in general information, technology and outcome. This makes an objective assessment of nations and projects possible.

4 Conclusions

In this paper we showed that comparing project dealing with E-Voting cannot be done without considering the context in which they are situated. Furthermore the identification of a national level and a project level makes the assessment of E-Voting initiatives much easier as well as the introduction of four dimensions technology, law, politics and society shows great potential to explain certain specifics of E-Voting projects that could not be explained otherwise. It would be very interesting to conduct a major analysis of European E-Voting projects based on these proposed dimensions.

5 Acknowledgements

We greatly appreciate the help of Nadia Braun that helped us with her enthusiasm and expertise and made this work possible. We also thank Bjoern Heppner for his preparatory work.

References

[Astr01] Aström, J., Should Democracy Online be Quick, Strong, or Thin? Communications of the ACM 44(1), 2001.

[AuFr04] Ausmann, R., Fremgen, G.: Internet und Politik - Der Nationalrat. Diploma Thesis, Vienna University of Economics and Business Administration, Vienna, 2004.

[CG04] Cap Gemini Ernst & Young: Webbasierte Untersuchung des elektronischen Service-Angebots der Öffentlichen Hand, 2004. Available online at http://www.at.capgemini.com/servlet/PB/show/1289862/eEurope4_DE.pdf accessed on 2004-04-10.

[Kers04] Kersting, N.: Online-Wahlen im Internationalen Vergleich. Aus Politik und Zeitgeschichte, pp. 16-23, B18/2004, Bonn, 2004.

[KaRu03] Karger, P., Ruess, O.: Sicherheit is conditio sine qua non. In: Braun, N., Heindl, P. et.al. E-Voting in der Schweiz, Deutschland und Österreich, Working Paper 2/2003 Institute for Information Processing and Economics, Vienna University of Economics and BA, Vienna, 2003.

[LeSv02] Leenes, R., Svensson, K.: Adapting E-voting in Europe: Context matters. Proceedings of EGPA, 2002.

[LeSv03] Leenes, Ronald, Svensson, Jörgen, ICT in the voting process – A report on 17 european countries, University of Twente, 2003.

[LuRe04] von Lucke, J., Reinermann, H.: Speyerer Definition von Electronic Government, 2004. Available at http://foev.dhv-speyer.de/ruvii accessed on 2004-04-28.

[MacA03] Macintosh, A.: Working Group 4 to the European Commission, Brussels, 2003. Available at http://www.eu-forum.org/summit/docs/WG4e-democracy-FINAL%20RESULTS.doc accessed on 2004-03-05.

[MoBa03] Moosmann, R., Baumberger, P.: eVoting-Sicherheitskonzepte – eine vergleichende Studie. In: Brücher, Heide: E-Government Präsenz 2/2003, Zeitschrift des Institut für Wirtschaft und Verwaltung, Bern, 2003.

[PaSe03] Parycek, P., Seeboeck, W.: Elektronische Demokratie: Chancen und Risiken für Gemeinden. In: Prosser, A., Krimmer, R.: E-Democracy: Technologie, Recht und Politik, OCG publication #174, Vienna, 2003.

[Scho04] Scholl, Jochen: E-government: A Special Case of ICT-enabled Business Process Change. 36th Hawaiian Conference of System Sciences (HICSS36), 2003.

Electronic Voting in Europe

E-Voting: International Developments and Lessons Learnt

Thomas M. Buchsbaum[1]

Expatriates Division
Federal Ministry for Foreign Affairs
Ballhausplatz 2
A-1014 Vienna, AUSTRIA
thomas.buchsbaum@bmaa.gv.at

Abstract: Countries worldwide are carrying growing interest in e-voting. The paper gives a brief overview on recent developments. The countries are joined in their interest by industry and international organisations. All three groups of actors - and individual actors within each group - have different and sometimes diverging reasons for their interest, and thus different goals. The paper focuses on remote / i[nternet]-voting. Member states of the Council of Europe (CoE) are in their final phase of standard-setting on e-voting. The paper provides a preview on a possible CoE recommendation. As the number of e-voting tests is growing, so are the lessons learnt. The paper contains a list of suggestions on ways how best to introduce (remote) e-voting.

1 Growing attention to e-voting

E-Voting has been attracting considerable attention during the last years. This fact is based on the one hand upon interest and attention devoted to e-government, e-democracy, e-governance, etc. On the other hand, interest in e-voting is founded in problems with domestic election systems, e.g. lacking flexibility with respect to timeframes and physical accessibility of polling stations, which progressively prevent citizens to cast their vote at these places.

Interest in e-voting exists in various quarters: government, parliaments, electorate, academia and industry - with each having sometimes conflicting interests. They can differ with respect, e.g., to speed, *individual* leadership, safety, user friendliness, etc.

[1] Thomas M. BUCHSBAUM, Dr.iur. (Vienna), MPhil (Cantab.), an Austrian career diplomat, is currently head of division (expatriates as well as property, social and labour issues) at the Austrian Federal Ministry for Foreign Affairs. The opinions expressed in this paper reflect his personal views.

E-voting is, however, no main priority of governments, even of those which are at the forefront of implementing e-government. It is not even mentioned in the EU *eEurope* action plans. International institutions started involvement in e-voting as well. While the Council of Europe (CoE) has taken the lead, elaborating legal, operational and technical standards, the EU has been focusing on supporting small pilots as well as financing targeted research. International QUANGOs, too, are active in the field.[2]

A generally accepted understanding of e-voting, let alone such a definition is missing. The same applies to remote e-voting. The term e-voting is being used from casting the vote by electronic means to asking the internet community for an opinion on a political issue, as well as from tabulating the votes by electronic means to integrated electronic systems from voters' and candidates' registration to the publication of election results. Other terms, like e.g. e-elections and i-voting have been introduced in order to clarify the specific contents of e-voting. The term e-voting should encompass only political elections and referenda, not initiatives or opinion polls or selective citizens participation between elections or referenda (e-consultations).

In general, two main types of e-voting can be identified

- e-voting supervised by the physical presence of representatives of governmental or independent electoral authorities, like electronic voting machines at polling stations or municipal offices, or at diplomatic or consular missions abroad; and

- e-voting within the voter's sole influence, not physically supervised by representatives of governmental authorities, like voting from one's own or another person's computer via the internet (i-voting), by touch-tone telephones, by mobile phones (including SMS), or via Digital TV, or at public open-air kiosks - which themselves are more venues and frames for different machines, like, *e.g.*, PCs or push-button voting machines, with or without smart card readers.

By this summary categorisation, advance voting of some Nordic countries at postal offices, or kiosk voting at municipal offices can fall, according to specific circumstances, in both of the above cases.

This paper will focus mainly on remote and internet e-voting.

Remote e-voting links the possibility of quick and reliable counting to that of voting outside of polling stations and traditional polling times as well as to the possibility of voting from abroad irrespective of locations of diplomatic and consular missions as well as unreliable postal services.

i-voting is of special interest to study as it is both most globally and convenient to use as well as most challenging with respect to legislation, technology and operation, and to understanding and trust by the electorate.

---

[2] *e.g.* the *Association of Central and Eastern European Election Officials (ACEEEO)*

As a working hypothesis, remote e-voting, *i.e.* casting an e-ballot without the physical supervision of a government official, can be regarded in many instances, from a legal perspective, similar to postal voting, as remote e-voting represents only a different channel of transmission of the ballot: the ballot is transmitted by electronic means instead of by post. There are, however, some differences in particular in the technical domain, *e.g.* on the audit trail and the scale of possible breakdowns.

Concluding this introduction, the author proposes to regard remote e-voting as a means by which government / administration can and indeed should provide citizens with an easier access to government services (e-administration, e-government) and thus enhance the possibilities for citizens' participation in democratic decision-making (e-democracy, e-governance).

2 An international overview

A number of countries, worldwide, has started or considered starting thinking and experimenting as well as implementing e-voting. In Europe, a variety of e-voting schemes is developed, tested and piloted across the continent. Outside of Europe, e-voting at polling stations is widely practised in the USA and Brazil - progressively followed by Mexico and considered by other Central and Latin American countries -, in some countries of the former Soviet Union and in India.

The reasons for the growing interest in e-voting may not be identical in all cases. In the draft CoE Recommendation, the following reasons are listed:

- enabling voters to cast their vote from a place other than the polling station in their voting district;
- facilitating the casting of the vote by the voter;
- facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;
- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;
- increasing voter turnout by providing additional voting channels;
- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;
- delivering voting results reliably and more quickly; and
- providing the electorate with a better service in pursuit of democracy, by offering a variety of voting channels.

As early developments with e-voting are well documented, we will concentrate in the following brief overview of individual countries on developments in 2003 and early 2004.

Germany started e-voting tests and pilots already in 1999, and is steadily continuing them, only at non-political/parliamentary elections, like at universities - students' bodies elections (Osnabrück, Bremerhaven) -, at local advisory level - youth community and senior citizens councils - as well at public and private employees councils. An elaborate set of - governmentally commissioned - requirements for on-line election systems is expected in the first half of 2004.

Switzerland - a country where postal voting is widespread because of the high number of referenda put to the electorate - has been undertaking remote e-voting pilots at local level, with respect to referenda, using different methods, and may enlarge the number of persons and types of polls involved, in the coming years - before deciding if e-voting will be definitely introduced. The conduct of e-referenda in 2003 and 2004 in Anières, Cologny and Carouge (a suburb of Geneva) has attracted considerable participation - higher than expected - as well as international attention. [Gen04]

The United Kingdom has been piloting, *inter alia*, i-voting at a large scale at municipal level, primarily in England, and *was* expected to extend these pilots at the 2004 EP election to a few million electors. While already in July 2003 the *Electoral Commission* stated that "we are clearly some way from the prospect of an e-enabled general election" and requested from government a road map and changes in legislation as well as a focus on electronic voting kiosks [UKEC03], in its recommendation for the electoral pilots at the 2004 elections, it did not recommend that an e-enabled element be included in any pilot schemes, as no region was ready for such innovation [UKEC04].

All French expatriates residing in the USA were given the possibility to validly elect via the internet their representatives to the French 'High Council of French Citizens Abroad' (*Conseil supérieur des Français de l'étranger - CSFE*), a public law body designating 12 members of the Upper House of Parliament (*Sénat*), in May 2003. This was well taken up and led, amongst other consequences, to a marked reduction of work by French consulates on election day - more than half of the votes were cast electronically in any district - but not to a general rise in participation [CSFE03].

Spain, too, has started testing e-voting in polling stations, kiosks and via the internet, in 2002, *inter alia*, through a 'body salinity identification'. An i-voting test for Catalonians abroad, in parallel to the November 2003 election to the regional parliament was conducted in Argentina, Belgium, Chile, Mexico and the USA. Participation was high (730 persons) and all requirements plus additional advantages were met [SCYT03]. Furthermore, on 14 March 2004, on the occasion of parliamentary elections, voters of three municipalities (Lugo (Mosteiro-Pol), Zamora and Toro (Zamora)) were given the possibility to test i-voting with smart cards after having cast their votes at a polling station. The Spanish Ministry of Interior stressed in its report the extraordinary acceptance of this channel by the population, the high number of participants, the ease in using the system and the necessity to legislate in this direction. [MinE03]

In the USA, the *Secure Electronic Registration and Voting Experiment* SERVE [SERV04], designed for expatriates participation in the US presidential elections of November 2004, was shelved in spring 2004 based upon a report or four members of a review group financed by the Department of Defence. They recommended shutting down the development of SERVE immediately and expressed the view that there "is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough" [JRSW04] The pilot was initially directed towards 1 million overseas electors, of whom 100.000 were expected to participate.

Since 2000, Ireland was carefully planning and testing kiosk e-voting for introduction at *all* polling stations at the EP and local elections of 11 June 2004, by a system which has been in use for years in two other European countries. Based upon a critical paper by two scientists [McGi03], reinforced by opposition action, and finally upon the negative "interim" report of a government-sponsored independent *Commission on Electronic Voting* [CEV04], e-voting at polling stations was not introduced for the mid-2004 elections.

The Netherlands – besides its traditional e-voting at polling stations – decided to run valid pilots on i-voting and telephone voting at the EP elections of mid-June 2004, also from abroad, while e-voting at polling stations would be eased. This country, thus, remained the only country, which was willing to conduct an important e-voting pilot in the course of the year 2004.

Italy and France have been testing an e-voting system in polling and police stations on small scale, with smart cards and fingerprint recognition, and which will be tested again in both countries at the EP elections of 2004 where the elector can choose to vote for the MEPs of the country of residence or of citizenship. From a technical point of view, this method could also be used on private internet computers.

On the project side, Slovene and Hungarian draft provisions for e-voting were elaborated which, in 2003, did not find the approval of the respective parliament. The Czech Republic may test e-voting in 2005/06.

Estonia, having the legal provisions already in place, is planning to pilot (advance) i-voting with smart cards and electronic signatures, at local elections in autumn 2005, with tests in autumn 2004.

3 The Austrian case

In Austria, like in many countries, too, e-voting is not a first priority of the government. The reasons for this state of affairs in Austria are varied: first of all, the Austrian Federal Constitution sets as election principles one more than the international "average" of the universal, equal, free, secret and direct suffrage [EC02]. It adds the personal exercise of the vote. In addition to this constitutional requirement, on the one hand, election provisions need a qualified - two thirds - majority in Parliament to be adopted. On the other hand, the Federal Constitution Court held in 1985 that postal vote was contrary to Austria's Constitution.[3] According to that decision, the physical presence of the voter appearing before a governmental authority is required.

A first test of remote e-voting by internet was undertaken *in parallel* to the elections of the *Austrian Federation of Students*, in May 2003, at an institute of the Vienna University of Economics and Business Administration, by a team of scientists led by Alexander Prosser, of Vienna University of Economics and Business Administration, which had developed the e-voting system used, itself.

As the *Austrian Federation of Students* is a public law body, its elections are governed by federal legislation. For such elections, as for those of the Federal Economic Chamber, legal provisions for e-voting already exist – while e-voting (like remote voting by post) is currently excluded for elections of the first layer in Austria, *i.e.* those of the head of state, the federal parliament, regional state parliaments and the European Parliament as well as for referenda.

According to reports by the organisers the i-voting test at the Vienna University of Economics and Business Administration was a complete success. [PKKU03] Out of 979 eligible persons, 355 e-"votes" were cast – which represents a participation rate (36,3%) which was 40% higher than those who cast paper ballots at polling station (25,9%). The - political - "results" were similar to the votes cast on paper ballots.

On May 13, 2003, the Austrian Federal Council of Ministers approved an *e-government strategy*. This decision includes a provision that Austria will attempt to be ranked amongst the top five countries in a benchmarking on the EU *action plan eEurope 2005*. In the annex by the Foreign Ministry to the government strategy on e-government, e-voting is listed as a project. [EGOV03]

[3] G18/85, VfSlg. 10.462

On July 29, 2003, a number of Austrian academics, including Prosser's team, presented during a meeting with the media, well reported, the request for creating the political and legal frames for e-voting in Austria, given its technical feasibility, and presented an *action plan for e-voting* [OCG03]. It contains a 4-step-approach, by which target groups for e-voting should be identified - first with respect to elections with small participation, including by Austrian citizens residing abroad - and the legal bases (re)considered; the necessary infrastructure requirements be created (including a centralised electronic voters register, the 'citizens card' designed according to data protection requirements, and the availability of the 'citizens card' assured to the target groups[4]); then a number of tests as well as pilot elections be conducted in order to accumulate the necessary information and feed-back; and finally the legal frame be adapted according to the necessities for e-voting in Austria.

Additional movement on discussing e-voting in Austria was brought in summer 2003 by the setting up of the 'Austria Convention' (*Österreich-Konvent*) - somehow similar to the past EU Convention - which is tasked to overhaul the Austrian constitution, and which included election issues including e-voting in its work programme.

The Austrian *Federal Act on E-Government* [EGOV04] entered into force on March 1, 2004, and provides - besides the residents' register - for the setting up of a *supplementary electronic register*. In order to electronically prove their identity, persons who are not included in the residents register, the commercial register or the associations register, can be registered in the *supplementary register* upon their request. To this end, data similar to those for residence registration are required.

In the explanatory memorandum to this Act, the provision mentioned above is explained as "*a first step towards enabling Austrian expatriates in a further future e.g. to be given the possibility of casting votes at Austrian elections in electronic form."*[5]

Following-up to the first test on remote e-voting by internet in parallel to the elections of the *Austrian Federation of Students* in 2003, the same project team conducted a second test of its system in parallel to the Austrian presidential elections of 25 April 2004,[6] amongst the 20.000 students of the Vienna University of Economics and Business Administration. 1.786 students participated, and the political result was extremely similar to that of all Austrian voters. [PKKU04]

In late spring 2004, the Federal Ministry of Interior established a working group on e-voting with broad participation, in order to study and establish a report, on various aspects of e-voting.

---

[4] A massive roll-out of these smart cards is foreseen from mid-2004 onwards first by banks (exchange of ATM cards) and later followed by social security institutions when the Austrian social security cards will be issued.

[5] explanatory memorandum to the (government) bill, in German:
http://www.bka.gv.at/datenschutz/v3/egov_erl.pdf accessed on 2004-03-30)

[6] At the presidential election, participation by expatriates while being the highest so far at any presidential election, declined with respect to the previous parliamentary election. Of those expatriates who are - optionally - registered with Austrian embassies and consulates and regularly informed on elections procedures, only one quarter has registered as voters, of which only one third participated in the elections. These voters represented 7,6 percent of those registered as expatriates at embassies and consulates, and 4 percent of the estimated total number of all Austrian expatriates.

4 Council of Europe's standard-setting

In addition to e-voting activities by countries, the most remarkable development on e-voting by international organisations is the standard-setting exercise within the framework of the Council of Europe (CoE). Upon initiative of the UK and a few other member states, the CoE took up the issue of e-voting as first and so far only international institution to do so in depth. The CoE has such not only the first right but also - so far - the monopoly on this issue – from an international organisation's perspective.

After a brainstorming meeting of national experts on 21 and 22 November 2002 [CoE02], terms of reference were adopted for an intergovernmental committee of experts[7] charged to develop an "*intergovernmentally agreed set of standards for e-enabled voting, that reflect Council of Europe member states' differing circumstances and can be expected to be followed by the ICT industry*" in the form of a draft Recommendation for adoption by the CoE Committee of Ministers.

Two meetings of the expert group were held in 2003 and two are scheduled for 2004, bringing the work of the group to a close in summer 2004. Two sub-groups - one on legal and operational standards (EE-S-LOS), and the other on core technical standards (EE-S-TS) - held meetings in between those of the (plenary) expert group.

The governmental experts' work proved to be much more difficult than initially expected. Different countries had - besides different voting schemes, different basic views on e-voting, different definitions of e-voting, different experiences with e-voting and experts with different expertise - different expectations for the expert group to deliver. Issues of levels of security, legal vs. technological leadership, government vs. industry orientation, and technological neutrality were repeatedly at the heart of the discussion. Quick progress was also hindered by specific existing election provisions in one or very few countries which were not only substantially different from those of others but seemed in some instances contrary to the commonly accepted European election standards. The main challenge, however, well mastered, was the necessary close co-operation of and mutual understanding between, legal and technology experts, on almost any issue of e-voting. On the other hand, the number of countries engaged in the whole process was small. While on legal and operational issues, possibly only a dozen or even less (of the 45) member states was continuously participating in the discussion, on technical issues the number was even smaller than that.

---

[7] *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting (IP1-S-EE)*

The probable outcome of this work will be intergovernmental standards, which will serve as *minimum* standards for legislation and product requirements for member states and for third parties, in particular the ICT industry. E-voting may in the forthcoming Recommendation be broadly defined as e-election or e-referendum that involves the use of electronic means in at least the casting of the vote. Numerous provisions in the draft Recommendation relate to e-elections in general, which are understood as political elections in which electronic means are used in one or more stages. On a possible definition of *remote* e-voting, consensus was evolving on e-voting where the casting of the vote is done by a device not controlled by an election official. The Recommendation will most probably not contain a view on the usefulness or necessity to introduce e-voting but an *indicative* list why individual countries are embarking on a course towards e-voting. In the legal and operational field, starting from and based upon, relevant international obligations and commitments, only e-voting specific provisions will be included.

5 Lessons learnt

On lessons learnt from e-voting tests, a division into a number of categories of cases may be useful:

- early (private) pilot projects (EC-funded)[8];
- countries hastily trying to introduce e-voting (H, SLO, US, …);
- academic work and its field tests (D, A);
- election administrations of countries, regions or municipalities with advanced pilots (CH, UK).

On lessons learnt from these e-voting events, a number of reports are available and need a comparative analysis. To this, the problems arisen within the CoE standard-setting exercise may be worth analysing as well, in order to draw conclusions for individual countries' or possible harmonised e-voting.

Other lessons are those learnt from legal expertise of national or international bodies. Here, the French National Commission on information technology and fundamental rights - *Commission nationale de l'informatique et des libertés (CNIL)* - has to be mentioned. It issued a recommendation on the safety of e-voting systems on 1 July 2003 [CNIL03], based upon two decisions on individual cases on the admissibility of e-voting systems. Focus is given to requirements on the technical side including specific requirements that a system must be able to prove *ex post*.

Besides a German set of - governmentally commissioned - requirements for on-line election systems expected in the first half of 2004, the Geneva "11 commandments for internet voting" are of special interest as they incorporate experiences with i-voting:

---

[8] papers and links via the EC-sponsored *eDemocracy Seminar* (Brussels, 12-13 February 2004): http://europa.eu.int/information_society/programmes/egov_rd/events/edemocracy_seminar/agenda/index_en.htm

(1) Votes cannot be intercepted nor modified;
(2) Votes cannot be known before the official ballot reading;
(3) Only registered voters will be able to vote;
(4) Each voter will have one and only one vote;
(5) Vote secrecy is guaranteed; it never will be possible to link a voter to his/her vote;
(6) The voting website will resist any denial of service attack;
(7) The voter will be protected against identity theft;
(8) The number of cast votes will be equal to the number of received ballots;
(9) It will be possible to prove that a given citizen has voted;
(10) The system will not accept votes outside the ballot opening period;
(11) The system will be audible. [Chev03]

On the compatibility of remote voting and electronic voting with the standards of the Council of Europe, the *European Commission for Democracy Through Law (Venice Commission)* has issued a report in spring 2004 [ECDL04]. According to its conclusions, remote voting is compatible with CoE standards if certain preventive measures are observed. For non-supervised e-voting, in order to be compatible with CoE standards, the system has to be secure and reliable. To this end, technical standards must overcome threats different from those existing with postal voting, the secrecy and transparency of the system being keys to that goal.

6 How best to introduce e-voting

While the following cannot be exhaustive or argued in detail here, we wish to present a few suggestions how best to introduce (remote) e-voting.

- suggest e-voting as additional, optional voting channel;
- start with identifiable group(s) of persons who wish / *need* e-voting, *e.g.* persons away from polling stations on election day(s), handicapped and bedridden persons incapable of going to polling stations, and mobile and busy people unwilling to go to polling stations but interested in participating in elections;
- go for added-value schemes which may be different in individual countries, with respect to *existing* voting channels and procedures;
- full understanding and trust by voters and lawmakers - including of the opposition[9] - are absolutely necessary;
- only a step-by-step approach leads to success: *election tests* separate from or parallel to, elections are to be held *before* valid *test elections (pilots)* can be, and small *before* big numbers of electors should be involved;

[9] In May 2004, five of the ten registered political parties in Kazakhstan requested the postponement of the introduction of e-voting because it was regarded by them as premature "when the transparency of voting with regular ballots has not been guaranteed … and creates conditions for various manipulations" (Interfax 21.05.04 09.57 MSK).

- in countries where postal voting is practised, extending postal voting to remote e-voting eases the introduction of e-voting;
- the best, as most reliable way, is identification with the help of electronic signatures / smart cards (not PINS);
- in order to avoid risks through postal transmissions, *any* transmission related to e-voting shall be possible / offered by electronic channels.

7 Conclusions

No universal trend towards a definite introduction of e-voting can be detected, not even by countries where first steps were undertaken on such a way.

Countries which hastily tried to implement large-scale e-voting without sufficient testing and public debate witnessed effective resistance by various quarters.

The implementation of e-voting has been undergoing ups and downs recently, from which, respectively, conclusions have to be drawn in order to introduce e-voting correctly and effectively.

In many countries considering the introduction of e-voting, legal, technological and political challenges still have to be solved and overcome, and this step, once achieved, subsequently explained to the interested public.

Meaningful advances on the way to e-voting can be achieved - besides trans-border exchange of views and experiences - only by close co-operation of and mutual understanding between, first of legal and technological experts, then by lawmakers and experts, and finally by politicians, experts and the public.

References

[CEV04] Commission on Electronic Voting: Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Dublin, 2004, available at http://www.cev.ie/htm/report/V02.pdf accessed on 2004-04-01.

[Chev03] Chevallier, M.: *Internet voting: Status; perspectives and Issues*, ITU E-Government Workshop, Geneva, 6 June 2003, available at: http://www.geneve.ch/chancellerie/E-Government/doc/UIT_6_6_03_web.ppt accessed on 2004-04-02.

[CNIL03] Commission nationale de l'informatique et des libertés (CNIL): Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, http://www.cnil.fr/index.php?id=1356&delib[uid]=12&cHash=d4482266b8 accessed on 2004-03-10.

[CoE02] Council of Europe: *Meeting of the national correspondents on e-voting,* Meeting Report, CoE doc. no. IP1 (2002) 29e fin

[CSFE03] Conseil supérieur des Français de l'étranger – CSFE: *Rapport du Directeur des Français à l'étranger et des étrangers en France, 2003*, Ministère des affaires étrangères, Paris, 2003.

[EC02] European Commission for Democracy Through Law: *Code of Good Practice in Election Matters,* October 2002, CoE doc. no. CDL-AD (2002) 23

[ECDL04] European Commission for Democracy through Law (Venice Commission), *Report on the Compatibility of Remote Voting and Electronic Voting with the Requirements of the Documents of the Council of Europe*, on the basis of a contribution by Mr. Christoph Grabenwarter (substitute member, Austria), 12-13 March 2004; Doc. CDL-AD(2004)012 – http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.pdf available on 2004-04-02.

[EGOV03] Chief Information Office, *e-government strategy* of the Austrian government and explanatory text (in German only), Vienna 2003, available at www.cio.gv.at/service/conferences/graz_2003/e-Gov_Broschuere.pdf accessed on 2004-02-10.

[EGOV04] *Federal Act on Provisions Facilitating Electronic Communication with Public Bodies (E-Government Act),* http://ris1.bka.intra.gv.at/authentic/findbgbl.aspx?name=entwurf&format=html&docid=COO_2026_100_2_30412 (official publication, in German) - the official text in English: www.ris.bka.gv.at/erv/erv_2004_1_10.pdf accessed on 2004-02-10.

[Gen04] The Geneva E-Voting Project, http://www.geneve.ch/chancellerie/E-Government/e-voting.html accessed on 2004-05-04

[JSRW04] Jefferson D.; Rubin A.D.; Simons B.; Wagner D.: *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, January 20, 2004, available at www.servesecurityreport.org accessed on 2004-03-30.

[McGi03] McGaley M.; Gibson J.P.: *Electronic Voting: A Safety Critical System*; Department of Computer Science, National University of Ireland, Maynooth, March 2003, www.cs.may.ie/research/reports/2003/nuim-cs-tr-2003-02.pdf, accessed on 2004-03-30.

[MinE03] Ministerio del Interior, Dirección General de Política Interior, Subdirección General de Política Interior y Processos Electorales*: Electronic voting trials using internet at the general election held on March 14 in Spain*, *Nota informativa*, Barcelona, 2003.

[OCG03] Austrian Computer Society (OCG): E-Voting Action Plan, text in German, Vienna, 2003, available at http://www.e-voting.at/main.php?ID=58 accessed on 2004-02-10.

[PKKU03] Prosser, A., Kofler, R., Krimmer, R., Unger, M.: First Internet Election in Austria, Vienna, 2003, available at http://www.e-voting.at/main.php?ID=53,

[SCYT03] SCYTL: *Elections to the Parliament of Catalonia 2003, Report on the Remote Electronic Voting Pootl*, Scytl Online World Security, Barcelona, 2003

[SERV04] SERVE USA: Internet Voting Project, 2004. http://www.serveusa.gov/public/aca.aspx, accessed on 2004-04-15.

[UKEC03] The Electoral Commission: *The shape of the elections to come*, London, 2003.

[UKEC04] The Electoral Commission: The Electoral pilots at June 2004 elections, 2004, http://www.electoralcommission.gov.uk/templates/search/document.cfm/8941 accessed on 2004-04-30.

E-Voting: Switzerland's Projects and their Legal Framework – in a European Context

Nadja Braun

Swiss Federal Chancellery
Bundeshaus West
CH-3003 Bern, SWITZERLAND
nadja.braun@bk.admin.ch

Abstract: Firstly, the reader is introduced to the Swiss political system, which can be described as a federalist state with direct democracy. Secondly, the Swiss e-voting pilot projects will be presented, against the background of the political system. Switzerland runs three pilot projects in order to test the feasibility of e-voting. In a third part the legal framework of e-voting in Switzerland is highlighted. In a fourth part the work of the Council of Europe is addressed. A last part contains Recommendations to the Swiss legislator. Today, the legal scheme allows for pilot projects. Should e-voting be introduced in Switzerland, the legal basis has to be adapted, taking into account the experience acquired through the pilot projects, and the Council of Europe's Recommendation on e-voting.

1 Introduction

1.1 Switzerland – a federalist state with direct democracy

Switzerland is well known for its direct democracy. All Swiss citizens over the age of eighteen[10] may take part in elections to the National Council (main chamber of the Federal Parliament) both actively and passively. They may also cast their vote in popular ballots.[11] A referendum[12] is compulsory for all amendments to the Constitution and for membership to some international organisations.[13] A vote must be held in such cases. In addition, voters have the right to initiative[14] and referendum[15], which means that they

[10] Except for those who have been incapacitated on grounds of mental illness or mental disability. See article 136 I of the Swiss Federal Constitution.
[11] Article 136 II of the Swiss Federal Constitution.
[12] A referendum (in the Swiss context) means: Popular vote by means of which voters can decide on, i.e. accept or reject, new or amended constitutional provisions, federal acts, and certain other decrees of the Federal Assembly.
[13] See article 140 of the Swiss Federal Constitution.
[14] See articles 138 and 139 of the Swiss Federal Constitution. Citizens may seek a decision on an amendment they want to make to the Constitution. For such an initiative to take place, the signatures of 100,000 voters must be collected within 18 months.
[15] See article 141 of the Swiss Federal Constitution. Federal laws, generally binding decisions of the Confederation, international treaties of indefinite duration and international treaties providing for the accession to an international organisation are subject to an optional referendum: in this case, a popular ballot is held if 50,000 citizens so request. The signatures must be collected within 100 days of a decree's publication.

can request a popular vote by collecting the requisite number of signatures. At present Swiss voters go to vote at the polls on polling weekends or in many places, depending on the local regulations, they can also cast a *postal vote,* i.e. they fill out their ballot paper before the polling weekend at any place outside the polling station and the vote is transmitted by ordinary mail.

Switzerland is a federalist state with 26 cantons and around 3'000 communes. *At least four times a year there are popular votes* in Switzerland on the national, cantonal and communal level. The four voting weekends and the intense political discussion on issues put to the vote in the run up to these votes are a particular feature of Switzerland.[16]

2 Swiss e-voting considerations

Switzerland is considering the question, whether e-voting should be introduced as an additional form of voting. The considerations in Switzerland are focused on *remote e-voting*, i.e. casting a vote from any PC that is connected to the internet or from mobile phones. The notion of e-voting includes casting a vote in *elections and referenda as well as the electronic signature of initiatives, requests for referenda and candidate proposals* for the election of the National Council.[17]

2.1 Why is Switzerland considering e-voting?

The new information and communications technologies and especially the internet have already changed the face of everyday and indeed political life. Political information is increasingly being offered and obtained over the internet. The changes in the information and communication habits have a significant impact on political discussions and efforts to mobilise the public. These changes are happening very fast whether or not e-voting is introduced. The Swiss Government wants to keep pace with these changes.[18] Young people, in particular, will perhaps soon come to see it as "old-fashioned" if they can do everything through the internet and yet not be able to cast their vote electronically. The reasons for considering e-voting in Switzerland include[19]:

- bringing political procedures in line with new developments in society
- making participation in elections and referenda easier
- adding new, attractive forms of participation to the traditional forms
- possibly increasing voter's turnout
- better protection of the democratic principle "one person – one vote" against traditional abuse

[16] For further information on Swiss Democracy in English see [L98].
[17] [B02], p. 646.
[18] [B02], p. 653.
[19] cf. [B02], p. 646+647.

One of these reasons is of special interest: the possibility of increasing voter's turnout with e-voting. Before considering this question (2.3), the Swiss scheme of pilot projects must be presented (2.2).

2.2 The three pilot projects

E-voting is a joint project of the Confederation and the cantons. The cantons are the main actors in the running of Swiss referenda and elections. This is why the necessary e-voting trials are carried out in three cantons that have volunteered to participate.[20] Two are French-speaking cantons, Geneva and Neuchâtel, and the third is a German-speaking canton, Zurich. Up to 80% of the trials are funded by the Confederation and the results will then be made available to all other cantons.[21]

The pilot projects in the three cantons should be completed by summer 2005 and then be evaluated. The political question as to whether and when e-voting will actually be introduced will subsequently be discussed and decided in the appropriate competent bodies, in the government and in the federal parliament.

2.2.1 Geneva: Three real e-votes[22]

Geneva has the most advanced pilot project. The cantonal administration, in partnership with Hewlett Packard and Wisekey of Geneva, developed an e-voting application. The system is based on existing voting materials and does not require any special features on a voter's computer. Swiss registered voters already receive their voting card and postal ballot by mail before every election. The card must be presented when voting or sent with the postal ballot by mail. Geneva added a scratchable field to the voting card that contains a personal ID code. When voting on the Internet, a voter uses this code to be recognised as an authorised voter by the Geneva servers. The voter then submits his/her vote and confirms or alters the choice before confirming his/her identity once again. This time the voter enters his/her date of birth and commune of origin, which are difficult to guess or counterfeit. The system then confirms that the vote has been successfully transmitted and recorded.

The electronic ballot is encrypted and sent to one of three servers, each one running on a different operating system. The votes are then forwarded to an electronic ballot box in a centralized location. Two keys are necessary in order to open the electronic ballot box.

---

[20] See survey among all the cantons http://www.admin.ch/ch/d/egov/ve/dokumente/umfrage.pdf
[21] Further information on the organisation of the Swiss e-voting pilot projects is available on: http://www.admin.ch/ch/d/egov/ve/index.html.
[22] For further information on the e-voting project in Geneva see: http://www.geneve.ch/chancellerie/e-government/e-voting.html.

To ensure security, the keys are given to members of different political parties that are represented in parliament. Since a voter's identity and ballot are kept in two distinct files, it is not possible to match a ballot and a voter. Geneva also carried out several hacking tests that showed the system to be very safe. Furthermore, any voting card with a scratched-off field is automatically rendered invalid for voting in person or by mail unless it can be proven that the voter tried to vote electronically but for some reason was unsuccessful. This can be confirmed by voting officials online or on lists distributed to voting stations. E-voting lasts 3 weeks and ends the day before the election or referendum.

The first regular referendum at which e-voting was allowed, took place on 19th January 2003 in the small commune of Anières. A second regular referendum with e-voting took place on 30th November 2003 in the commune of Cologny and the third regular referendum with e-voting was carried out on 18th of April 2004 in the city of Carouge.[23] Among the next steps, Geneva is planning to use e-voting within the national referendum on the 26th of September 2004 which has to be allowed by the Swiss Federal Council.

2.2.2 Neuchâtel: e-voting as part of a secure one-stop e-counter[24]

This pilot project will use a different approach to e-voting and should be ready for its first test during a national referendum in June 2005. Close collaboration between the canton and its 62 communes has given way to the creation of a "virtual government window" – the "guichet sécurisé unique". This window is an information network resulting from the shared management of voter registration lists and communications infrastructure. Similar to Internet banking today, canton residents will receive a user-ID and password to enter the one-stop e-counter, which offers many other government services. Before each popular vote, voters will receive an additional code that will allow them to cast their electronic ballot.

2.2.3 Zurich: Tackling the problem of decentralised voter registers[25]

Zurich has 216,000 registered voters divided into small communes of in some cases less than 200 voters. Each commune uses its own information system, manages its own registered voter's lists and counts its own votes. For this reason, this project will be the most ambitious one. Because voting is carried out at the canton and commune levels, close cooperation between all levels of government is vital for success. The plan is to implement e-voting at the commune level and have the communes pass on the results to the canton. Zurich is creating a canton-wide shared database of voters that will constantly be updated by the communes, whilst hardly changing the existing network of information systems in the communes. The first test during a national referendum is scheduled for the beginning of 2005.

---

[23] For details on voter turnout during these three referenda with e-voting see below §2.3
[24] For further information on the e-voting project in Neuchâtel see: http://www.ne.ch/gvu/.
[25] For further information on the e-voting project in Zurich see:
http://www.statistik.zh.ch/projekte/evoting/evoting.htm

2.3 Enhancement of voter turnout

Wherever e-voting is tested and implemented, there are a lot of expectations that voter participation will be raised.[26] In Switzerland this expectation exists as well and the experience with the introduction of postal voting in 1994 shows that this expectation is to a certain extent justified.[27] However, two expert opinions come to different results. The Research and Documentation Centre on Direct Democracy (C2D) comes to the conclusion that participation in the canton of Geneva could be raised by 9%[28]. Another study analysing voter participation within Switzerland comes to the conclusion that e-voting would raise voter participation by less than 2%.[29] Both studies date from the year 2001 – a time where e-voting had not yet been tested during a regular referendum. Meanwhile three referenda have been held with e-voting in the canton of Geneva. It is therefore interesting to look at the voter participation in those referenda:

Anières (19.01.03): Voter participation was raised by 13,8%[30]:

Registered voters	**Votes cast**	**Participation**	**Average participation in Anières**	**Votes cast with e-voting**	**Remote votes (postal votes and e-voting)**
1'162	741	63,8%	50%	43,6%	93,5%

Cologny (30.11.03): 28,9% of the votes cast were cast over the internet.[31]

Registered voters	**Votes cast**	**Participation**	**Average participation in Cologny**	**Votes cast with e-voting**	**Remote votes (postal votes and e-voting)**
2'523	1'495	59,3%	no indication[32]	28,9%	66,8%

Carouge (18.04.04): 25,9% voters cast their vote using the internet.[33]

Registered voters	**Votes cast**	**Participation**	**Average participation in Carouge**	**Votes cast with e-voting**	**Remote votes (postal votes and e-voting)**
9'049	3'978	43,9%	no indication	25,9%	95,2%

[26] See e.g. [C04]
[27] [B98].
[28] [AT01], p. 54.
[29] [L01], p.6.
[30] [RA03].
[31] [RC03].
[32] Since 1980, Cologny did not have any referenda exclusively on topics of the communal level. Therefore no comparative data exists.
[33] [RC04].

On the basis of the data collected during the three referenda using e-voting, the conclusion can be drawn, that e-voting has the potential of rising voter turnout. However, the data is not sufficient in order to give any indication as to what extent participation could be enhanced. A second conclusion that can be drawn is, that where voters have the possibility of using other remote voting channels, e-voting is not the most popular channel. Traditional remote voting channels seem to be preferred.

3 Legal Framework

3.1 The legal provisions for the testing of e-voting

The paramount concept in Switzerland can be summarised as follows: e-voting has to be as secure and reliable as the traditional voting methods (i.e. postal voting and voting at polling stations). In order to make sure, that e-voting complies with all the existing provisions that rule traditional elections and referenda, articles 27a-27q of the Order on Political Rights[34] contain detailed requirements. The cantonal e-voting projects have to comply with these requirements in order to use their e-voting system for carrying out national elections and referenda. An e-voting system has to ensure, inter alia:

- that only entitled voters may take part in the ballot
- that each voter shall have a single vote and shall vote only once
- that it is impossible for any third parties systematically to intercept, alter or divert electronic votes or decisively influence the result of the ballot
- that it is impossible for any third parties to find out the content of the votes cast
- that all the votes cast are taken into account when the votes are counted
- that any systematic fraud is impossible

Special attention has been given to the principles of secret and of free suffrage.

3.2 Secret suffrage

The Order on Political Rights contains various requirements that have to be fulfilled in order to safeguard the principle of secret suffrage. *First* of all, the measures taken to ensure that votes remain secret must guarantee that the responsible authorities will receive only those electronic votes which have been made perfectly anonymous and which cannot be traced in any way.[35] *Secondly*, the transmission of electronic ballot papers, the monitoring of voter status, the recording on the electoral roll of the casting of each person's vote and the depositing of the ballot in the electronic ballot box must be so designed and organised that it is impossible at any time to identify any voter's vote.[36]

---

[34] Verordnung über die politischen Rechte; available on the internet under http://www.bk.admin.ch/ch/d/sr/c161_11.html
[35] Article 27f of the Order on Political Rights.
[36] Article 27f of the Order on Political Rights.

The Swiss legislation requires *thirdly* an encryption during the whole voting process, i.e. ballot papers must be encrypted at the very start of the procedure when the vote is submitted and they must be transmitted in encrypted form.[37] The votes cast shall be decoded only when they are to be counted.[38] As a *fourth* requirement, every measure must be taken to ensure that no link can be established between a ballot paper cast in the electronic ballot box and the voter casting it.[39] *Fifthly,* applications connected with electronic voting must be clearly separated from other applications[40] and *sixthly*, while an electronic ballot box is open, any intervention affecting the system or one of its component parts must be carried out by a minimum of two people, must be the subject of a report and must be able to be monitored by representatives of the responsible authority.[41] As a *seventh*, general requirement, every measure must be taken to ensure that none of the information needed during electronic processing can be used to breach the secrecy of the voting.[42] *Eighthly*, during the electronic voting process, there must be no intervention unconnected with the voting which is under way affecting either the ballot and election server or the electronic ballot box server.[43] *Ninthly*, the legislation requires that the votes cast must be stored randomly in the electronic ballot box. The order in which the votes are stored must not make it possible for the order in which they arrived to be reconstituted.[44] Furthermore, the legislation states in a *tenth* requirement, that the instructions for the machine used for the voting must indicate how the user's vote may be deleted from all the said machine's memories.[45] *Finally,* the vote must disappear from the screen of the machine used by the voter to cast the vote as soon as that vote has been sent and the software used must not enable the votes cast to be printed.[46]

3.3 Free suffrage

Different provisions deal with the ensuring of this principle. In order to guarantee free suffrage, *firstly*, the machine which the voter is using to vote must advise him/her that his/her vote has reached its destination.[47] *Secondly*, the encryption of the data transmitted must be so designed as to ensure that no electronic ballot paper which has been altered will be counted.[48] *Thirdly*, the way in which persons using electronic voting are guided through the procedure must not be such as to encourage them to vote precipitately or without reflection.[49] As a *fourth* requirement, the legislation states, that before voting,

---

[37] Article 27f of the Order on Political Rights.
[38] Article 27f of the Order on Political Rights.
[39] Article 27g of the Order on Political Rights.
[40] Article 27g of the Order on Political Rights.
[41] Article 27g of the Order on Political Rights.
[42] Article 27g of the Order on Political Rights.
[43] Article 27h of the Order on Political Rights.
[44] Article 27h of the Order on Political Rights.
[45] Article 27h of the Order on Political Rights.
[46] Article 27h of the Order on Political Rights.
[47] Article 27e of the Order on Political Rights.
[48] Article 27e of the Order on Political Rights.
[49] Article 27e of the Order on Political Rights.

voters must have their attention explicitly drawn to the fact that, by submitting their vote by electronic means, they are playing a valid part in a ballot.[50] *Fifthly*, it must not be possible for any manipulative message to appear during the process of electronic voting on the machine being used by the voter to cast the vote.[51] *Finally,* as they vote, voters must be able to alter their choice before submitting their vote, or to break off the procedure.[52]

4 The work of the Council of Europe

Within the Integrated Project "Making democratic institutions work", the Council of Europe has mandated a Multidisciplinary Ad Hoc Group of Specialists[53] with the task to draft legal, operational and technical standards for e-enabled voting. The result of this work will be a Recommendation which will be adopted by the Committee of Ministers in autumn 2004.[54] The Recommendation consists of a set of legal and operational standards and core technical requirements for e-voting. The legal standards are intended to apply the principles of existing Council of Europe and other international instruments in the field of elections to the circumstances of e-voting.

4.1 Legal standards

In this article the legal standards, i.e. those standards relating to the legal context in which e-voting is permitted, are of special interest.[55] The legal standards follow the pattern of the five basic principles of democratic elections and referenda: universal, equal, free, secret and direct suffrage.[56] These five principles are equally applicable to e-voting as to traditional elections or referenda. However, specificities of e-voting do not give rise to issues to the same extent in relation to all of the five principles. Whereas for the principles of universal, equal, free and secret suffrage special provisions with regard to e-voting are made, the principle of direct suffrage is not addressed. The legal standards also contain a set of procedural safeguards to ensure that all five basic principles of democratic elections and referenda are implemented and maintained with e-voting. Out of this set of standards, three will be highlighted and discussed below:

1. Standard no I,4[57]: *"Unless channels of remote e-voting are universally accessible, they should be only an additional and optional means of voting."*

---

[50] Article 27e of the Order on Political Rights.
[51] Article 27e of the Order on Political Rights.
[52] Article 27e of the Order on Political Rights.
[53] The author of this article was a member of the Swiss delegation to this group.
[54] [C04].
[55] The legal standards can be found in Appendix I to the Recommendation.
[56] In 2002, the European Commission for Democracy through Law (Venice Commission) has adopted a non-binding Code of Good Practice in Electoral Matters(Opinion no. 190/2002) in which these five principles are identified as the fundamental rules underlying Europe's electoral heritage.
[57] The numbering refers to the draft Recommendation from 29.3.04.

This provision is to protect the voter from a situation where the only means being offered for voting is one that is not effectively available to him/her. Adding additional electronic voting channels to traditional forms of voting may make elections and referenda more accessible. However, the drafters of the Recommendation suppose that using a single electronic voting channel in isolation restricts accessibility. This is one of several provisions in the Recommendation, in which the drafters have consciously been careful not to endanger the five above mentioned principles. However, they take into account the possibility that future developments in technology might lead to a change of these provisions.

2. Standard no I,20: *"Member states should take steps to ensure that voters understand and have confidence in the e-voting system in use."* and no I, 21: *"Information on the functioning of an e-voting system should be made publicly available."*

Confidence by voters and candidates in the voting system(s) used is essential not only to participation but also to the democratic system as such. The drafters of the Recommendation agree that only the understanding of the e-voting system(s) can be the basis for this confidence. There were long discussions on the level of understanding of the e-voting system. Traditional voting methods are simple and well tried. Voters are familiar with voting systems using ballot papers and ballot boxes and understand the general rules that govern how they should vote and how their vote is collected and counted unaltered. The introduction of e-voting produces a new situation in which voters will be less familiar with the system and perhaps less able to understand it. Confidence can be enhanced by providing to the voters as much information as possible with regard to the technique, which is being used for e-voting. However, unless a voter has specific technical knowledge, he/she may never be able to understand the system in the same way as he/she understands a traditional voting system.

3. Standard no I, 24: *"The components of the e-voting system should be disclosed, at least to the competent electoral authorities, as required for verification and accreditation purposes."*

The drafters agreed that the correct functioning of e-voting and the maintaining of it's security are essential. There was some debate on how these aims could be achieved. While some clearly preferred to mention that the system suppliers had to disclose the source code of their system, others preferred a more general requirement which demands the disclosure of the critical elements of the system. The standard takes into account both reflections. The "components of the e-voting system" include, for instance the design of the system, detailed documentation, component evaluation, certification reports, in-depth penetration testing as well as the source code.

5 Conclusion: Recommendations to the Swiss legislator

The experience gained in the three pilot projects and the Recommendation of the Council of Europe have to be taken into account when drafting future legislation on e-voting. The Recommendation does not contain any provisions contradicting the current Swiss requirements for e-voting. However, there are some provisions that are worth being integrated in a future Swiss legislation on e-voting, for instance standard no I, 22: *"Voters should be provided with an opportunity to practise any new method of e-voting before and separately from the moment of casting an electronic vote."* Although the pilot tests provide an opportunity for the voters to practise e-voting, a future introduction of e-voting in Switzerland would have to be accompanied by measures ensuring that voters have trust and confidence in the system. The possibility of practising is a very good way of enhancing this confidence.

Another standard which should be integrated into a future legislation on e-voting in Switzerland is standard no I, 27: *"The e-voting system should not prevent the partial or complete re-run of an election or a referendum."* Whereas this requirement can already be deducted from existing electoral legislation in Switzerland, it is nevertheless worth mentioning in the context of e-voting. Indeed, if a re-run of an election or referendum becomes necessary, the re-run may not be possible without the support of the e-voting system used in the original election or referendum, even if this e-voting system is not to be used in the re-run itself.

Finally it can be said that the work on e-voting is an ongoing process. The legislation has to be continuously reviewed and adapted to developments in technology.

References

[AT01] Auer A./Trechsel A. (Research and Documentation Centre on Direct Democracy , C2D): Voter par Internet? Le projet e-voting dans le canton de Genève dans une perspective socio-politique et juridique de l'introduction du e-voting dans le canton de Genève. Geneva, Novembre 2001; available on the Internet under: http://www.admin.ch/ch/d/egov/ve/dokumente/dokumente_beilagen/e_auer.pdf.

[B98] Bundeskanzlei: Umfrage über die briefliche Stimmabgabe, November 1998, available at http://www.bk.admin.ch/ch/d/pore/va/doku/pdf/enquete_bsa.pdf

[B02] Bericht über den Vote électronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte vom 9. Januar 2002, Bundesblatt 2002, S. 645-700 (BBl *2002* 645). Available at http://www.admin.ch/ch/d/ff/2002/645.pdf.

[C04] Council of Europe: Draft Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting; 29th March 2004; available at http://www.coe.int/t/e/integrated_projects/democracy /02_Activities/02_e-voting/02_Draft_Recommendation/

[L98] Linder, Wolf: Swiss Democracy: possible solutions to conflict in multicultural societies, 2nd ed., New York 1998

[L01] Linder, Wolf: Gutachten zum e-Voting, Bern September 2001; available at: http://www.admin.ch/ch/d/egov/ve/dokumente/dokumente_beilagen/e_linder.pdf.

Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions

Bernard Van Acker

IBM Global Services Belgium
Generaal Lemanstraat 69
B-2018 Antwerpen, BELGIUM
Bernard_Vanacker@be.ibm.com

Abstract. This paper, useful to anyone who has to address the public and representatives of the world of politics, focuses on the specific topic of resistance to vote-coercion. By using a model, we want to illustrate the implicit – and possibly realistic - assumption that vote-buying is not profitable or doable in current conditions. But these assumptions do not necessarily hold good in all environments. For those environments, recent - mainly cryptographic - publications show that coercion-resistant remote e-voting schemes are indeed possible.

1 Introduction

Throughout this e-Voting conference, the main requirements that any election should satisfy, will have been mentioned sufficiently; they are summarised well in article 21 of the Universal Declaration of Human Rights, which encompasses: the privacy of the vote, the accuracy of the count, the principle of one man, one vote, the freedom of vote.

As has also been mentioned many times, if we introduce remote e-Voting, we will drastically change the implementation (i.e. procedures) of elections, but there is a general consensus that the principles themselves should be strictly safeguarded.

One major concern that the political world has expressed on various occasions when talking about remote voting is that of vote coercion.

1.1. Definition

Coercion occurs when the vote is not free, i.e. when the voter is forced or bought into voting for an option which he would not have chosen had he not been under pressure or if he had not been offered a bribe.

[JJ02] has broadened the definition of coercion somewhat with forced abstention (a voter is forced into not turning out to vote), randomisation (a voter is forced into casting a random vote) and simulation (the coercer can impersonate the voter and thereby cast a vote in his or her place).

Vote coercion is by no means the only way a dishonest candidate or other party might alter the result of the elections: others are the bullying (or eliminating) of other candidates, or controlling the media. But these aspects are not specific to remote e-Voting, so we shall leave them out of scope.

1.2. Contingency under current legislation.

Under traditional voting methods, (1) the secrecy of the vote is guaranteed and (2) it is ensured furthermore that voters cannot prove to anyone else how they have voted. The second measure is followed very strictly: for example, a simple erasure on a paper ballot will render that ballot invalid[58]. The reasoning is that such an erasure could be a means by which the voter can prove how he/she voted.

1.3. Relevance for remote e-Voting schemes

Exposure to the risk of vote-buying is an argument used in public debates against remote voting procedures.

As an illustration, a citation of the republican Livingston in 1994 before the US Subcommittee on elections59 : "Telephone voting conjures up endless images of interest- groups paying armies of volunteers or goons to go out on the street, enter people's homes and intimidate or otherwise deprive them of their franchise in order to have people vote for a candidate for whom that they might otherwise have had no intention of voting."

Until recently, there seemed to be a consensus that remote e-Voting schemes offered little or no protection against vote coercion. This, together with the forecast costs of projected pilots, caused some initiatives to be broken off in the Netherlands around the end of 2001, beginning of 2002 [EPN02][60].

As we shall see below, this changed a few years ago, and positive proposals are now available.

---

[58] Example in Belgian legislation of local elections: Article 51 Loi électorale: « Ceux dont la forme et les dimensions auraient été altérées, qui contiendraient à l'intérieur un papier ou un objet quelconque ou dont l'auteur pourrait être rendu reconnaissable par un signe, une rature ou une marque non autorisée par la loi. »

[59] before the US House of Representatives, committee on House Administration, Subcommittee on Elections, on 22nd September 1994.

[60] A new pilot, restricted to Dutch citizens residing abroad, has been launched since then and is scheduled for use in the European elections in June 2004.

2 The risk and the impact of voter coercion

In an attempt to rationalise the discussion about the risk of vote coercion, we shall present here a rough-and-ready economic model. The aim here will be only to *define* both the presence of a risk and the impact of vote coercion,[61] and in this way identify the factors that might have an effect on them.

2.1. Rough economic model: Supply ad demand of votes.

A. the model.

The model will acknowledge that a candidate has a "default popularity" that will not depend on the resources (time & money) he puts into his/her campaign. But on the other hand, the model will allow those resources to affect the result somewhat in either of two ways:

- either by persuading voters to vote for the candidate voluntarily
- or to buy/coerce voters into voting for the candidate against their will.

The above distinction is important. A candidate who relies solely on persuasion doesn't need any proof to make sure that someone voted for him; on the other hand, coercion requires the ability of voters to prove how they voted. We will return to this point later.

We distinguish two kinds of players:

1) a candidate or party who is looking for votes, and who has at his disposal a number of resources, which may be time and/or money, of either himself or one of his supporters

2) the voters, for whom we take the original voter's preference as our starting point.

Throughout this description, we shall make the following assumptions:

1) The budget (the resources in terms of time and/or money) at the disposal of the candidate is fixed in advance[62].
2) A section of the electorate will not change its mind. Two categories here:
    a. Voters who were going to vote for the candidate anyway.
    b. Voters who would never vote for the candidate, no matter what the resources put in place to persuade, buy or coerce them into voting that way.

---

[61] Much more advanced models of the electoral market exist, which are outside the scope of this paper and can be found elsewhere, for example Besley, T. and Coat, S., "An Economic Model of Representative Democracy", Caress Working paper 95-02, 1995, 44p.

[62] Observed on at least one occasion: local elections 2000, Belgium. Also, in Belgium, budgets are restricted by law.

We will now describe two scenarii.

The first scenario makes the assumption that was implicitly made in Switzerland when introducing the first remote e-Voting scheme in 2003:

- The cost of persuading a voter into voting is less than the cost of coercing voters. This can be defended in countries with a high standard of living (we shall call this “the Swiss model”);

In the second scenario, we shall make the opposite assumption and see what the consequences are.

In the first scenario (”the Swiss model“) illustrated in figure 1, we distinguish two groups that may be influenced:

- The voters who did not originally intend to vote for the candidate, but who might be persuaded to vote voluntarily; this is illustrated by the green area in the colour picture).
- The voters who originally did not intend to vote for the candidate, cannot be persuaded to vote voluntarily; but who might be coerced into voting for the candidate. This is illustrated by the orange area in the picture below.

Remember that the curve can, and will, shift left or right dramatically, depending on the popularity of the candidate or party, which is desirable in free and fair elections anyway.

If we add up the costs, and look at the *total cost* of paying to get a certain number (percentage) of votes, we get indeed the following illustration.

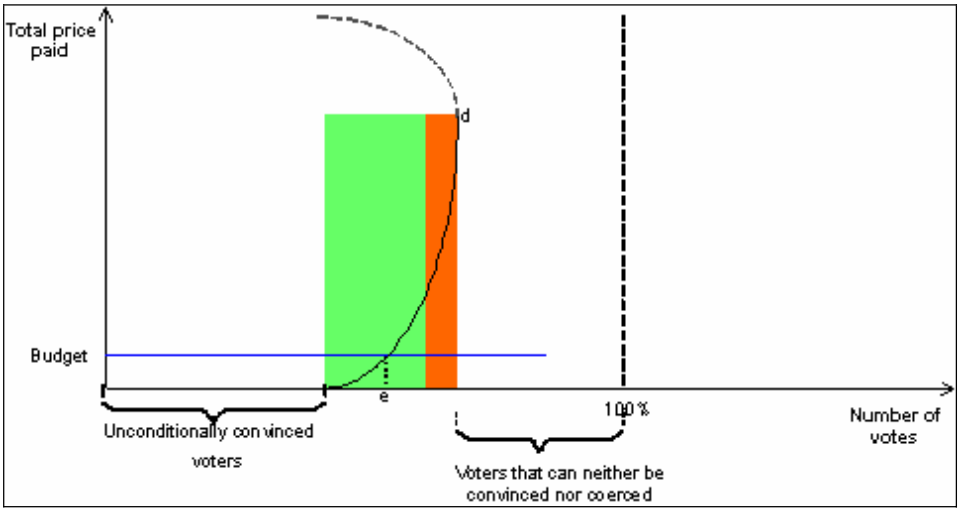


Figure 1: The total price of paying to get a certain result, versus a given budget (Swiss model).

If coercion is too blatant and so becomes too obvious, this may have a negative effect on the preference of even voters who were originally in favour of the candidate. We illustrate this by the dotted line starting from point d; the shape and position of that line are purely illustrative.

In this simple model, the candidate can keep "paying for" votes, either by persuasion or by coercion, until the total price to be paid equals his budget. This is illustrated by the intersection of the black line and the blue (fixed budget) line, which gives e votes (see point e on the X axis).

In figure 1 (illustrating the "Swiss model" scenario), the intersection occurs at the area of voters who can still be persuaded. In that example, no coercion has taken place.

In this "Swiss model", many politicians will recognise the situation: if they had more money and – more importantly - *time*, they would spend it all on the yet-to-be-convinced citizens, i.e. by persuasion. The idea of coercion wouldn't even cross their minds. A slight opportunity might exist among groups who support the candidate, but who lack rationality (e.g. very young supporters).

But in other situations, the "Swiss model" (the assumption that the cost of coercing people would be greater that that of persuading them) may be invalid, for example in unstable countries or situations. In the second scenario, the illustrative graph might very well look like figure 2 below:

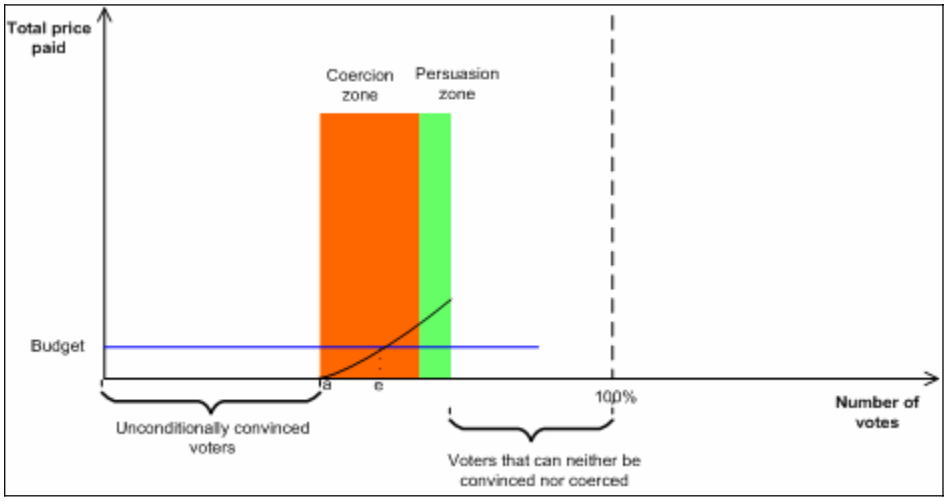


Figure 2: The total price to be paid for a certain result, versus a given budget (non-Swiss model).

In this scenario, the most "efficient" way of spending one's budget is to coerce a number of voters (by vote-buying or otherwise).

B. Influencing Factors

B.1. Probability-influencing factors.

For coercion to be an option, and hence a non-zero risk, one of the following should apply: (a) we are in a non-Swiss scenario as illustrated in figure 2, (b) in the Swiss model, the number of persuadable persons is smaller and (c) in the Swiss model, the curve representing the total cost is flatter in the persuasion area.

All this assumes no negative impact on popularity due to coercion itself (remember: illustrated by the dotted line starting from point d).

B.2. Impact-influencing factors.

In the figure 2, the impact of coercion was the segment between a and e, and has obviously been influenced by the slope of the curve between a and e.

The higher the cost of coercion (represented by an upward shift of the cost curve in the coercion zone), the smaller the impact of coercion, even if there is a risk. The same is true for both the Swiss and the non-Swiss model.

This is also true for a lower coercion effectiveness (represented by a leftward shift or rotation of the cost curve). This will be discussed extensively below.

a) The budget.

If the budget is low, the impact (coercion or persuasion) is smaller anyway. This is relevant where budgets are limited by law, as in Belgium.

This model was mentioned just to rationalise the discussion, not to give an economic "justification" of remote e-Voting systems.

2.2. Practical risks with traditional voting methods

Under traditional voting methods, the voter hides himself physically from any witnesses to cast his vote. Various officials are present to ensure that the vote is secret, that no proof of the vote is taken and that no one steals the vote. A risk that remains is the use of long lists[63], on which one can give preference votes to more than one candidate. In for example the local elections at Antwerp, the number of possible combinations was so large that one could have encoded a passport number in binary form, just by casting valid preference votes. No such abuses have been reported, however.

Another risk that remains valid is that of forced abstention, already mentioned above; this might be relevant in situations where violence is to be expected at polling stations; following our model this should increase risk and impact of it.

2.3. Practical risks with remote voting

When a vote is cast remotely, no witnesses are present to ensure voting freedom. Until recently, this led observers to believe freedom with remote voting was simply not possible. We will see some recent developments below that tend to show the opposite.

Force abstention persists here, with the difference that it will be more costly, since voters are scattered around remote locations; under our model, the impact should be lower here.

3 Contingency against coercion.

Contingency can act upon the cost or upon the effectiveness of coercion.

The cost of coercion can be increased – and hence our cost-curve in figure 3 shifted upwards - for example by requiring that a coercer be physically present, or by incorporating voting credentials into valued assets like identity cards, as mentioned in [Ch01].

---

[63] To be mathematically precise: where the lg (number of voters) is smaller than or equal to the number of candidates on one list. Example: 16,777,216 voters, and 24 candidates per list.

But effectiveness can also be reduced, and our cost curve in figure 3 thereby rotated leftwards. As we shall indeed show below, systems have been proposed that make it easy to lie about one's vote, and hence impossible for a voter to prove how he/she voted. In that case, offering bribes or threatening voters cannot make any difference to their voting behaviour, no matter what the budget spent. In our graph, the curve in the "coercion area" will then become ultimately a vertical line (as will the coercion area itself). Like [JJ02], we shall call such electoral systems "Coercion-Resistant".

In each of the three main categories of remote voting systems traditionally offered, namely[64] mixed nets using public key encryption like [Ch81; PO01], systems that rely on homomorphism like [CF85; Co86; Iv91] and systems that use blind signatures like [JL97; JLS99; KKP03], protection against coercion often remained unmentioned, or was indicated as being an open problem.

But in recent years, specialists in cryptography have been designing ways to vote remotely and/or electronically, while limiting the opportunity to prove to an outsider how the vote was cast.

Examples[65] are Hirt and Sako's method [HS00], Chaum's pre-encrypted ballots [Ch01], Chaum's coercion-free receipt [Ch03], and the planned system with loose sheets for the IBM social elections[66].

3.5. Further developments: Re-used voting booth secrecy.

With the above mentioned techniques, we have mainly limited the period during which coercion can take place, or made it more expensive, for example by requiring the physical presence of a coercer or vote- buyer at a given time.

Could we achieve the same level of coercion-resistance with remote voting as in a traditional voting booth?

An honest attempt to achieve exactly that will take into account the following comparison with remote authentication.

Remote authentication requires firstly an administration (registration authority) to invest time in verifying a person's true identity. Often this even requires the person to be physically present.

This "investment" brings benefits later on in remote electronic transactions when authentication is required. In other words, the fact of having been physically present once in the past is reused several times when remote authentication is needed.

---

[64] References are not exhaustive

[65] See http://home.tiscali.be/bernardvanacker/remoteVoting/CoercionFreeTechniques.html for a description of these alternatives

[66] The proposed system for the IBM social elections was using a scheme similar to the example in [MSV03];

We can imagine a similar investment for coercion resistance. We could devise a procedure to shield voters from anyone when they perform a secret action, for example by inviting the user to go into a booth (similar to a voting booth) at the site where also the authentication material is handed over.

Once outside the booth, he/she will not be able to prove anything about the secret action performed in the booth (eg whether or not he/she shuffled a pile of loose paper sheets containing both valid and invalid keys).

Under this scenario, the only option left open to a coercer would be to prevent the citizen from voting at all (the ”forced abstention attack“, supra), or to force him/her into voting randomly, which amounts to the same thing. Since this risk also exists with traditional voting methods, the protection against vote-buying would be the same as when voting at the polling station.

Of course, the citizen should remember well what he/she had done in private. This aspect and the aspect of user acceptance needs to be investigated, as has been done for the e-Voting pilot in Vienna [DPK03] and for in-booth electronic voting in Belgium [DKP03].

4. Conclusion

Firstly, we presented a model to help decide whether any anti-coercion measures were necessary.

For where required, we showed a few examples of ways to protect against voter coercion. We also said it ought to be possible to achieve the same level of protection for privacy and against voter coercion when using remote e-voting compared with when voting in person at the polling station. Essential here is the way keys are distributed. How readily users will accept these procedures and techniques remains to be investigated.

References

[Ch81] Chaum, D.: Untraceable Electronic Mail, return Addresses, and Digital Pseudonyms, Communications of the ACM 24, 2, (Feb. 1981), p 84-88;

[Ch01] Chaum, D.: Physical and Digital Secret Ballot Systems,patent application WO00155940A1 2001.

[Ch03] Chaum, David., "Secret-Ballot receipts and Transparent Integrity", 2003, available at www.vreceipt.com/article.pdf

[CF85] Cohen, J.D. and Fischer, M.J.: A Robust and Verifiable Cryptographically Secure election Scheme: Proceedings of IEEE Conference on Foundations of Computer Science, 1985.

[Co86] Cohen, J.D.: Improving Privacy in Cryptographic Elections: Yale University Computer Science Department Technical Report YALEU/DCS/ TR-454 , February 1986.

[DKP03] Delwit, P. ; Kulahci, E. ; Pilet, J-B.: Vote électronique et participation politique en Belgique: presentation at the Belgian Parliament in December 2003, available on http://www.belspo.be/belspo/home/publ/index_fr.stm

[DPK03] Dickinger, A.; Prosser, A.; Krimmer, R.: Studierende und elektronische Wahlen: eine Analyse; e-Democracy: Technologie, Recht und Politik. Prosser, A. and Krimmer, R., Oesterreicchische Computer Gesellschaft, 2003, pp 145-144.

[DO01] Dare, P.; Owlett, J.: Method and system for supply of data; UK Patent Office application 0126596.6, 2001;

[EPN02] EPN: Kiezen op afstand, dichterbij dan u denkt; EPN- Platform voor de informatiesamenleving, Den Haag, 2002; p 28 and 41.

[HS00] Hirt, M; Sako, K.: Efficient Receipt-free Voting, based on homomorphic Encryption, Eurocrypt 2000, 18p.

[Iv91] Iversen, K, R.: A Cryptographic Scheme for Computerized General Elections, Advances in Cryptology: Proc of Crypt '91, LNCS 576, Springer-Verlag, pp 405-419, 1991.

[JJ02] Juels, A ;Jacobsson, M.: Coercion-Resistant electronic elections, RSA Laboratories, 2002.

[JL97] Juang, W.S.; Lei, C.L.: A secure and Practical Electronic Voting Scheme for Real World Environments, IEICE Trans. on Fundamentals, Vol E80-A, No.1, , January, 1997., pp. 64-71.

[JLS99] Juang, W.S.; Lei, C.L.; Chang, C.Y.: Anonymous channel and authentication in wireless communications, Computer communications 22 (1999) p1502-1511;

[KKP03] Kofler, R.; Krimmer, R.; Prosser, A.:Electronic Voting: Algorithmic and Implementation Issues: Proceedings of the 36th Hawaii International Conference on System Sciences, 2003.

[MSV03] Marino, A.; Seliger, F.; Van Acker, B.: System for achieving anonymous communication of messages using secret key cryptography, patent application FR920030081, 2003.

E-Voting and Biometric Systems?

Sonja Hof

University of Linz, Austria
Institute of Applied Computer Science,
Division: Business, Administration and Society;
University of Linz, AUSTRIA
sonja.hof@ifs.uni-linz.ac.at

Abstract: As e-Voting gains more importance while practicable solutions are being implemented, more questions arise concerning alternative possibilities for a secure and feasible authentication. The specific peculiarities of secure authentication to a system are various and for a sensitive area like e-Voting also challenging. In this paper we evaluate biometric systems in order to prove their capabilities for e-Voting systems.

1 Introduction

This contribution tries to look into e-Voting from a different angle on the necessary citizen authorization from a different angle. Instead of concepts such as one-time passwords or smart cards, we try to look into the pros and cons of a biometric approach.

Biometrics is the science that tries to fetch human biological features with an automated machine either to authentication or identification [LA02]. Biometric products should remove the necessity of password or PINs. Typical two-factor authorizations use possession, e.g. smart card, and knowledge, e.g. PIN. Biometric systems try to exchange knowledge with an individual feature, e.g. finger print. Recording of the feature should be comfortable and fast. The most commonly use biometric feature is the finger print. It is well known and in wide spread use in daily police work.

In contrast to passwords or pin codes, biometric features are dynamic, i.e. they change over time. This is probably the most challenging property of the biometric system. One has to find a balance between a check which is too strict and generates too many rejections, and a check which is too loose and generates too many false accepts.

This paper gives an overview of biometric approaches to e-Voting. The first section gives an introduction into e-Voting. The second section elaborates on security issues specific to e-Voting systems. Finally, it focuses on security in e-Voting systems with biometric systems.

2 E-Voting

Many countries have started research projects or even pilots for e-Voting (UK [html5],[PKK03], ACM US [html6], NIST [html7], Austria [SM03], Switzerland [BR03],[html9],[html8], Germany [BR03]. There are two main motivations to introduce e-Voting: cost savings and increased voter participation and interest. Providing information and increasing the convenience for the citizens goes hand in hand, and it also offers disabled people the possibility to use e-Voting systems [html10]. Some approaches of putting e-Voting into practise are quite innovative, such as voting using SMS [html8] but still they have to cope with a lot of unsolved technical problems and therefore, it is doubtful if they will be implemented. The most sensitive aspects within e-Voting are fraught with secrecy and access issues.

3 E-Voting and Security

E-Voting is probably the most security sensitive process handled electronically nowadays [Cr02]. The main reason for this being that the worst-case scenario is really catastrophic. For example, assume an electronic vote for the German Bundestag is discovered to have been tampered with. This fraudulent act will not only have drastic consequences for Germany itself, but will also have enormous consequences for the whole European Union and further a field. Bearing this in mind, the highest achievable security is never too much for an e-Voting system.

Generally one can divide the requirements for an electronic vote into three basic musts:

- Do the actual laws in a given country allow for the electronic handling of votes?
- Does a technical solution exist that fulfils all the restrictions and requirements imposed on it by the corresponding laws?
- Do the actual voters desire and accept an electronic voting system and in particular, the designed voting system [Ba04] [Ev04]?

Fulfilling these requirements is quite challenge. Especially as their individual areas of expertise are different: law, technology and social science.

4 Biometric Identification in E-Voting

In this section, we will have a look at biometric systems [Zi03] focusing on their relevance for e-Voting systems. We will look at their different aspects regarding e-Voting systems, e.g. the huge number of persons using the biometrics or the small expertise of typical users.

Standard	Gegenstand
ISO/IEC FCD 7816-11	Personal verification through biometric methods
NISTIR 6529 (CBEFF)	Common Biometric Exchange Format Framework www.nist.gov/NISTIR-6529-CBEFF bzw. ~/cbeff [CBEFF is extended by NIST/Biometric Consortium Biometric Interoperability, Performance and Assurance Working Group (www.nist.gov/bcwg)]
XCBF	XML Common Biometric Format: XML-Schem to exchange biometric data via Internet www.oasis-open.org/committees/xcbf/
ANSI B10.8	Finger minutiae extraction and format standard for one-to-one matching
ANSI/NIST ITL 1-2000	Data format for the interchange of fingerprint, facial, and scar mark & tattoo (SMT)
ESIGN-K	EU standard for digital signature cards (PIN and biometric authentication) draft: www.ni.din.de/sixcms/detail.php3?id=389
DIN V64400	Finger minutiae encoding formats and parameters for on-card-matching
BDPP	Biometric Device Protection Profile (UK) www.cesg.gov.uk/technology/biometrics
FBPP	Federal Biometric Protection Profile (US-DoD) http://niap.nist.gov/cc-scheme/PP_BSPP-MR_V0.02.html
BioAPI(ANSI/INCITS 358-2002)	Consortium for standardisation of communication interface between application and biometric devices www.bioapi.com
HA-API	Human Authentication Application Program Interface: US Ministry of defence initiated project. It was merged after version 2.0 in 1998 with the BioAPI-Consortium.
BAPI	Biometric API von I/O Software: Proprietary biometric interface of Microsoft.

Figure 1: Biometric standardisation efforts (Source: heise.de)

One of the main issues we like to stress is the difference between biometric authentication compared to "classic" authentication as e.g. smart cards. In this comparison we ignore the well known concept of card readers based on biometrics, e.g. card readers with fingerprint authentication; In this case, the biometric input is not used to authenticate the user to the e-Voting system, but rather to authenticate his/her smart card. The e-Voting system does not interact in any way with the biometric characteristics of the actual users, but still authenticates the user with the help of the user's authentication certificate as present on the card. Seen from this perspective, this solution is not a biometric approach to e-Voting. From now on, we will focus on biometric approaches that actually use the biometric data to authenticate the e-Voting system. Another issue with biometric systems is their relative young age, there is still currently a set of standardisation efforts going on (see Figure 1).

We will first have a look at some of the possible biometric properties that can be used for the authentication of individual persons. In this paper, we will restrict ourselves to present just a subset of different biometric properties. We explicitly do not focus on their feasibility, but rather try to show the wide spectrum of "theoretically" possible human properties that can be used in biometric systems.

Fingerprint. Fingerprint scanners are probably the most commonly used biometric system; as and replace the pin code entry to unlock the card, especially in the area of smartcard readers. Similar systems include hand geometry or palmprints [html1] [html4].

Iris. Another static property of individuals are eyes. One can either use pictures of the person's iris or use a retina scanner that scans blood vessels to create an individual data set.

Face. The human face is also a feature that can be used by biometric systems. Human face recognition by analysing the size and position of different facial features is being pushed for use at several airports to increase security. Another possible approach is to make infrared recordings and analyse the resulting facial thermogram [html3].

Voice. A more behavioural individual aspect of humans are their voices. Everybody has a special mode and tone while speaking. Voice recognition tries to analyse these features and use them to identify a person [html2].

Signature. Another behavioural aspect of a person usable by biometrical analyses is the signature. Not only the form but also the dynamic aspects can be seen as a set of unique features of a person. Other possible movable biometric input could be the rhythm and pattern of a person's walk.

DNA analysis. Now this is a rather more theoretical idea for biometric identification. Imagine a DNA reader that can create a full DNA analysis within seconds from just a few cells of a person's body. Such a device would surely be a match to, e.g. a finger print reader, when comparing the quality of the results.

Multi-Biometric Systems. As a final approach to biometric data gathering, one can combine two or more actual biometric analyses and combine their results, i.e. use more than one uni-biometric system. This combination yields better results than each of the combined analyses individually and thereby increases the reliability of the biometric system.

With this we tried to give a quick introduction to the different kinds of biometric systems and will now focus on some of their technical aspects which are relevant to an e-Voting system. Initially, we will concentrate on the infrastructure required to use biometric input as the authentication means for an e-Voting system. As already mentioned before, we will not look at localized biometric measures, e.g. fingerprint scanner on the smart card reader that replaces the normal pin code, but focus on the truly biometric input to the actual e-Voting system.

If we look at such e-Voting systems, we need to have some type of central storage that handles the biometric templates of the users. This data storage again imposes high security demands, it must be impossible to tamper with the biometric templates, as this would enable fraud. An attack on the templates can come from two directions:

- A third party could replace a number of biometric templates against other templates which would allow them manipulate the results of the vote.

- Even if the risk of the above attack is seen as neglectable, there is one attacker that has a much more direct access to the biometric templates: the government. This opens a relatively straight forward route to manipulate the votes in a favourable direction for the currently governing party. One may state now that this is already possible – as many examples have unfortunately shown – even if using "old-style" paper votes.

However, the danger of this happening unnoticed is much larger. In a paper based voting scheme, large scale fraud involves a large number of people. Therefore, the risk of an information leak is several degrees higher than in an electronic environment where frauds on a similar scale can be executed in an automated manner by just a few people.

The two attacks mentioned above try to move the result of the vote into a direction favoured by the attacker. However, there is a second type of attack that is rather destructive. In this case, the goal of the attack is not to change the outcome of the vote, but rather to prevent a result of the vote in the first place. Again there are two possibilities for the attacker. Either, he starts the attack before the actual vote starts, or he initiates the attack after the vote has started, e.g. using distributed denial of service (DDOS) attack on the servers with the biometric templates. The second approach has two advantages. First, it gives the service provider of the vote a very limited time to react to the vote. Second, one has to take into account the psychological consequences such an attack has on a person not able to give his/her vote.

After taking a look at a selection of biometric properties, as well as the required infrastructure with its weaknesses, we will now set out a list of criteria that allows us to classify biometric systems.

Cost. The cost factor is very important for e-Voting systems as the number of participants tends to be very high. Each and every participant needs to spend an initial amount of money for his/her biometric reader. Depending on the recorded biometric characteristic, these costs can be rather large.

False Reject Rate (FRR). No biometric system is perfect. One of the problems that can occur are so called false rejects. A false reject is the situation where a valid user tries to authenticate and is falsely rejected by the system (see Figure 2).

One way such a false reject can happen is due to noise in the recorded biometric data, e.g. a fingerprint with a new scar or a voice altered due to a cold. Noise can also be introduced due to altered environmental conditions, e.g. humidity on a capacity finger print reader or unfavourable illumination for a face recogniser. If this "noisy" data is matched with the stored user templates, the difference can be too big and the authentication fails, i.e. the user is rejected.

Another issue with the universal applicability of biometric systems is the possibility that a user is not able to participate, as he/she does not have sufficient biometric properties within the measured domain, e.g. his fingerprints were burnt during a fire.

Final effects that may cause a false reject are time dependent variations either with the individual, e.g. tone of the voice changing over time or an accident that changes the individual's signature, or a variation due to the reader, e.g. a new version of the reader uses slightly different sensors that yield slightly different measurements.

	False Reject Rate	False Accept Rate
Fingerprint[1]	0.20%	0.20%
Voice[2]	10-20%	2-5%
Face[3]	10%	1%

Figure 2: FRR and FAR for three example biometric systems

If a biometric device is used as an access control mechanism, a false reject may be acceptable, as it may only require the user to use a different means of authentication, e.g. by calling security, to access the area from which he was excluded by the authentication system. In the context of e-Voting, a false reject means to deny an individual of the possibility to execute his/her right as a citizen. An e-Voting system using biometrics has to cope with such scenarios.

False Accept Rate (FAR). The second type of error a biometric system is doomed to make is a so called false accept. In contrast to false rejects, a false accept means that a user is successfully accepted (authenticated) even though he/she should have been rejected. In an e-Voting system there are actually two scenarios where we have to talk about false accepts (see Figure 2):

- An unauthorized user is erroneously accepted for a vote. This has two consequences. First, this user is able to give a vote and thereby to possibly change the vote's outcome. Second, as the wrongly authenticated user already gave his vote, the actual user that should be allowed to vote is wrongly rejected yielding the same result as with a false reject.

- An authorized user is confounded with another valid user. With this the short-term effect does not yield a wrong vote count. However, once the other user is trying to make his/her vote, he will be rejected under the assumption that he has already made his/her vote. This again leads to all the consequences of a false reject.

Another source of false accepts is the uniqueness of the tested biometric recordings. Even with assuming that a finger print is actually unique, a finger print reader will not yield different readings for all users. This stems from the fact that a finger print does not yield the complete finger print as a picture for matching against the stored template, but it actually reduces the input to a predefined feature set of typical characteristics. This introduces a theoretical upper boundary on the number of individuals that a biometric system can distinguish between.

Spoofing. Another important aspect of a biometric system is its susceptibility to spoofing. Spoofing is the wilful trail to impose a false accept onto the biometric system. This type of attack is especially relevant for behavioural properties, e.g. replay of a voice recording or a blueprint of a signature. However, face recognition as well as the other physical properties are also susceptible to this type of attack.

As an example we will examine an attack on finger print readers. Modern models do not rely solely on the pattern of the applied finger, but also executes a "Life-Check". [4] describes how members of the CCC try this approach. Their approach is to first get a finger print of the impersonated person using conventional means. This fingerprint is digitally photographed and reworked using graphics software and finally transferred onto a photo layered using acid. This form is then used to make a latex print of the original finger. Due to the very thin layer of latex, it is also possible to trick the "life-check" of the reader.

Costs of the Biometric Infrastructure. In addition to the costs of the biometric readers, the cost of the biometric infrastructure has to be handled. The infrastructure roughly consists of two parts: enrolment infrastructure and voting infrastructure. The enrolment infrastructure is necessary to collect and maintain a database of the biometric templates of all participants. The voting infrastructure handles the actual e-Voting process, i.e. it must be able to handle authentication requests of all participants within the official voting period; Depending on the used biometric mechanism which may require considerable space as well as computing power.

Another aspect of the biometric infrastructure is its high demand on security. It has to maintain the two requirements of a secure e-Voting system: personalisation and privacy. Each and every vote has to be linked to a person while preserving the person's anonymity of what exactly he/she voted for.

Fail Safety of Biometric Infrastructure. In an access control system, a failure of the system may be acceptable. There will be a way to bypass the system and go back to a manual authentication mechanism, e.g. using guards and controlling some form of paper ID. With an e-Voting system, this is not acceptable. Let's assume an ongoing one day vote from 8:00 in the morning to 2:00 in the afternoon. At 9:00, an attacker starts a DDOS attack on the biometric infrastructure that actually blocks it and denies most citizens to actually process their votes. In the best case, it may be sufficient to repeat the vote at a later time. However, in other scenarios, it may have much more serious consequences.

Scenarios, such as the one described with the DDOS attack are quite common nowadays. As e-Voting systems become more common and votes on larger scales are handled by them, the danger of such attacks becomes more and more imminent.

Acceptance of Biometric Infrastructure. The final factor for a biometric user authentication mechanism is its acceptance with its users. Voting is mostly a matter of trust. Regardless of its actual security, a voting system (electronic or not) is only as good as its acceptance with its users. Therefore, any introduction of a new voting system requires a good deal of work to increase its acceptance with the future users. This is especially true with biometric systems [Si02]. Increasing the acceptance of such e-Voting systems is probably a slow process.

5 Conclusions

Disregarding security, e-Voting systems can use biometric user authentication. However: Is this necessary? Is it worth the effort and are the security risks manageable? We cannot give an answer to these questions within the scope of this paper. We also cannot give an answer to these questions that is globally applicable. The main conclusion of this paper is that biometric approaches for e-Voting systems should be extremely carefully deployed. Actually, we would even recommend to refrain from using biometric systems in this context (at least for the moment). Currently, the rejection rates are just too high for an environment as sensitive as electronic votes.

Properties that have to be improved include:

- False accept rate
- False reject rate
- Protection against spoofing attacks
- Judicial aspects regarding access to biometric templates

References

[html1] Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2002/

[html2] The 2000 NIST Speaker Recognition Evaluation, http://www.nist.gov/speech/tests/spk/2000

[html3] Face Recognition Vendor Test, http://www.rfvt.org/FRVT2002

[html4] Latex versus Biometric, http://www.heise.de/ct/03/18/052/default.shtml

[html5] Implementing Electronic Voting in the UK, http://www.odpm.gov.uk/stellent/groups/odpm_localgov/documents/pdf/odpm_locgov_pdf_605188.pdf

[html6] USACM, Policy Brief: E-Voting Technology and Standards, http://www.acm.org/usacm/Issues/EVoting.htm

[html7] NIST Voting Standards Symposium, December 2003, http://realex.nist.gov/votingstandards/

[html8] http://www.swissinfo.org/sde/swissinfo.html?siteSect=2051&sid=1575998

[html9] http://www.revue.ch/de/content/fuenfte_schweiz/e_voting.php?navid_meta=3

[html10] Equal access to electoral procedures, Good practice guidance, http://www.electoralcommission.gov.uk/files/dms/GoodPracticeequalaccess-finalversion_11561-9041__E__N__S__W__.pdf

[Ba04] J. Bannet, D.Price, A.Rudys, J.Singer, D.Wallach, Hack-a-Vote: Security Issues with Electronic Voting Systems, IEEE Security & Privacy Vol2 Nr1 p32

[Br03] Braun, N., P. Heindl, et al. (2003). e-Voting in der Schweiz, Deutschland und Österreich ein Überblick. Arbeitspapiere zum Tätigkeitsfeld Informationsverarbeitung und Informationswirtschaft. Wien, Wirtschaftsuniversität. 2003,2.

[Cr02] Crown, e-Voting Security Study, Issue 1.2, 2002

[Ev04] D. Evens, N. Paul, Election Security: Perception and Reality, IEEE Security & Privacy Vol2 Nr1 p24

[La02] TeleTrust Deutschland, G. Lassman, Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, 2002, http://www.teletrust.de/down/kritkat_2-0.zip

[PKK03] Alexander Prosser, Robert Kofler, Robert Krimmer; Deploying Electronic Democracy for Public Corporations, proc. EGOV 2003, p234-239

[Si02] Richard Sietmann, Im Fadenkreuz: Auf dem Weg in eine andere Gesellschaft, http://www.heise.de/ct/02/05/146/default.shtml

[Sm03] Ella Smith, Ann Macintosh; E-Voting: Powerful Symbol of E-Democracy, proc. EGOV 2003, p240-245

[Zi03] Peter-Michael Ziegler, Europas größte Gesichtserkennungsanlage im Zoo Hannover, http://www.heise.de/ct/03/09/026/default.shtml

Security as belief
User's perceptions on the security of electronic voting systems

Anne-Marie Oostveen, Peter van den Besselaar

Department of Social Sciences, NIWI- KNAW
Royal Netherlands Academy of Arts and Sciences, The NETHERLANDS
{Anne-Marie.Oostveen | Peter.Van.den.Besselaar}@niwi.knaw.nl

Abstract In this paper a pilot e-voting system is being studied to gain insight into the complexity of IT security issues. The current debate about whether or not electronic voting systems need to have a verifiable paper audit trail provides the context of the paper. According to many researchers a voter-verified paper trail is the only way voters can have confidence that their vote has been recorded correctly. However, technologists start to acknowledge that security mechanisms are fundamental social mechanisms. Trust is of great importance; people no longer have a blind faith in scientific objectivity and the "experts". We examine the opinions of users involved in the testing of the TruE-Vote e-voting system, in particular concerning issues like security, verifiability and trust. The results do indeed suggest that IT security is more than just a technological issue.

1. Introduction

In an attempt to modernize our election process by moving from paper ballots towards the world of digital computers, governments might be jeopardizing our democracy. Many politicians and legislators are in favor of electronic voting. They see a lot of possibilities in this new technology. Most proponents argue that the adoption of e-voting systems would increase voter participation. Increasing voter participation is of interest because voter turnout has been low and declining in most countries. Election directors are also quick to pick up on the argument that electronic voting may be the cheapest, quickest and most efficient way to administer elections and count votes. However, the cost of online voting would vary enormously depending on the type of system employed and the type of security used [Co]. But from the first trials with e-voting, there has been a lot of concern about the security of computer-based voting systems. Online voting systems have a lot of technical vulnerabilities. Already in 2000 the California Internet Task Force concluded that the 'technological threats to the security, integrity and secrecy of Internet ballots are significant'. The general feeling was that although electronic voting is nice in theory, the security is still not sufficient. The British Independent Commission on Alternative Voting Methods also published a report recommending a delay of Internet voting until suitable security criteria are in place [Co].

Broadly speaking, each election involves four distinct stages: registration, validation, casting of the vote and tallying. Each of the stages can take place by using physical or electronic procedures. Computer-based voting systems need to satisfy a number of criteria like eligibility, uniqueness, accuracy, reliability, verifiability, secrecy, etc. to guarantee a democratic election which is free, equal and secret [IPI]. In this paper we focus on the criterion of verifiability. Public confidence in the election process depends on the verifiability of an election. There must be assurance that all votes cast are indeed counted and attributed correctly. As each vote is cast, an unalterable record must be created ensuring a verifiable audit trial. Electronic voting is likely to lead to changes in how the public maintains confidence in the integrity of elections. With e-voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process [IPI]. Media stories about security threats to the Internet have an immediate impact on public confidence and past failures have made people distrustful. Electronic voting may not achieve the goal of increasing turnout if voters do not trust it. There are many ways to make electronic voting more secure. Mechanisms that form the structure of security are for instance Personal Identification Numbers or passwords, encryption, digital signature, smart cards or biometric identifiers. It is important to make the voting and counting processes as transparent as possible. Trust in an electronic voting system means having confidence in the machinery and infrastructure, rather than simply in the physical and administrative processes. All non-free software is secret by nature and there is virtually no way to be sure that the software does not include a trick to change the results of the vote. As McGaley and Gibson (2003) point out, 'apart from the obvious requirement that the votes are tabulated correctly, it is vital that the votes are seen to be tabulated correctly. A voting system is only as good as the public believes it to be'. A way to provide a voter-verified audit trial (VVAT) was proposed by Rebecca Mercuri. Her method requires that "the voting system prints a paper ballot containing the selections made on the computer. This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises. If, for some reason, the paper does not match the intended choices on the computer, a poll worker can be shown the problem, the ballot can be voided, and another opportunity to vote provided." [Me]

Unfortunately, most of the e-voting machines presently used in different countries do not provide a paper trail that can be compared to the machine count, so a recount is as good as impossible. Bev Harris's research shows that there have been numerous voting machine errors. These errors came to light by accident when voters' rolls were compared with voter tallies and the numbers didn't add up. Harris says: "Because hardly anyone audits by comparing actual ballot counts with machine tallies, we are not likely to catch other kinds of errors unless something bizarre shows up" [Ha]. She continues to point out how frightening it is that for every machine miscount discovered, there must be a hundred that go unnoticed. This impossibility to find out whether a machine counted the votes accurately is a major security issue.

No matter how undisputable the importance of technological security solutions (like VVATs) are for gaining the trust of users, we think it is also indispensable to look at the more sociological issues that are at play. It goes without saying that a VVAT will improve the trust of people in e-voting systems, but history has shown us that trust in a

new technology alone is not sufficient for its success and adaptation. Neither can we state that trust in technology is always based on the actual state of the technology itself. In this paper we show that the opinion of users about the security of systems is often based on perception and not so much on actual facts. In other words, people will use insecure systems if they feel or think they are secure. They base this perception of security on things like: the reputation of the organizing institution, the attitude of the mass media, the opinions of friends and family and the convenience it will bring them. This paper tries to point out the importance of the sociopolitical context. Software may reduce the amount of trust you need in human beings, but as one moves about in the world, the sense of security, privacy and autonomy turns out to be "a function of social structures" [Ul]. This is an explorative study and it is not our goal to explain the opinions of users about the verifiability of the TruE-Vote system. We try to show that the belief in verifiability is not based on the technology itself but is more an issue of trust and opinions about new technology.

2. Voter-verifiable electronic voting

People should not just be able to vote, they should also have a voting system that can be trusted. If citizens don't trust that the elections they participate in are fair and the machines count correct than they will never accept that those votes represent their voice. It is therefore that computer scientists, social researchers and engineers are promoting a hybrid system. They favor touch screen machines with a voter-verified paper ballot, with an audit that compares the two against each other. With electronic voting systems there is always the risk that a program flaw or tampering with the software could change votes and even change the outcome of elections. These changes may not be detected because of the secrecy of the vote. Once the voter has cast his ballot and left the polling booth, no one will be able to detect or correct possible errors that the machine made in recording the votes. Computer scientists say that the solution is relatively simple; all voting equipment should require a VVAT which provides a permanent record of each vote. This way the voter can check to ensure that it represents their intent. It is vital that the voter doesn't keep the paper so that he can't prove to someone that he has voted a certain way and get paid for it. When there is any doubt about the results of the election, there is the possibility of a manual recount.

There are three reasons why the discussion about the security of electronic voting systems seems to have focused lately on the necessity of a voter-verifiable audit trail. First of all, the discussion got a great impulse after the Florida election debacle, when the Institute of Electrical and Electronics Engineers (IEEE) took up the question of standards for voting equipment. The IEEE created a working group, called Project P1583. Unfortunately, instead of using this opportunity to create a good national standard, which would set benchmarks for the security, reliability, accessibility and accuracy of these machines, P1583 created a weak standard that would have led to unsafe electronic voting machines [Ma2]. Even more problematic, the standard failed to require or even recommend that voting machines be truly verifiable, a security measure that has broad support within the computer security community. A number of respected scientists involved in electronic voting were so appalled by the proposed new standard

that they urged IEEE members and others to write to IEEE to express concern about the draft electronic voting machine standard. They warned that the future of democratic systems in the U.S. and around the world would be implicated by this standard. They stated: “We also support the idea of modernizing our election processes using digital technology, as long as we maintain, or better yet, increase the trustworthiness of the election processes along the way. But this standard does not do this, and it must be reworked.” [Ma2].

A second reason why more scientists started to worry about electronic voting systems without VVAT was the uproar about the Diebold voting system. Numerous reports have found Diebold machines and other computer voting systems vulnerable to error and tampering [KS; Ha; Ko; Ma1; Ma3]. In general, no one is allowed to see the code used by electronic voting machines. Computer scientist David Dill says that when he started asking questions about voting machines, he received answers that made no sense. “It is frustrating because claims are made about these systems, how they are designed, how they work, that, frankly, I don’t believe. In some cases, I don’t believe it because the claims they are making are impossible” [Ha]. Dill is limited in his ability to refute the impossible claims because of the secrecy of the data; machines can’t be examined and manuals can’t be looked at. Computer technician David Allen says: “These things are so secret we’re supposed to just guess whether we can trust them” [Ha]. But lo and behold! More or less by mistake Diebold published the source code on a public internet site. Harris discovered that Diebold’s voting software is so flawed that anyone with access to the system’s computer can change the votes and overwrite the audit trail without leaving any record [Ma3]. But someone could also get into the system by hacking the telephone system or by going backwards in through the Internet [Ma3]. This security flaw was already brought to light in October 2001 by Ciber Labs but Diebold did nothing to fix it. Even worse, a memo written by Ken Clark, an engineer at Diebold, says that they decided not to put a password on this system’s ‘backdoor’ because it was proving useful. Scientists at the Johns Hopkins University also found that the security in Diebold’s software was “far below even the most minimal security standards applicable in other contexts”. Their report shows that insiders as well as outsiders can do the damage [KS]. In reaction to the security issues identified by computer scientists, Diebold claims that the Johns Hopkins team is not familiar with the election processes, makes false technical assumptions, has an inadequate research methodology and makes insufficient use of input from election experts [Di; KS]. The voting machine vendors furthermore state that researchers should have reviewed all the different layers of security in voting systems together. Sequoia Voting Systems [SV] believes that: “Election security must be viewed as a combination of numerous layers of security that, taken individually may be insufficient, but taken as a whole, provide accurate, secure and accessible elections.”

The third reason why computer scientists doubt the trustworthiness of electronic voting machines without paper backups is the fact that computerized voting gives the power to whoever controls the computer [CC]. Lynn Landers writes: “Only a few companies dominate the market for computer voting machines. Alarmingly, under U.S. federal law, no background checks are required on these companies or their employees.” [La] Computer scientists and journalists question the political affiliations of the leading voting companies. Harris found that just before the 1996 election Senator Hagel, a

Nebraska Republican, used to run the voting company that provided most of the voting machines that count votes in his state. And he still owned a stake in the firm [Ha; Ma1]. Hagel failed to disclose his ties to the company whose machines counted his votes. Harris points out: “This is not a grey area. This is lying” [Ha]. Conflicts of interest are seen everywhere. Ohio’s newspaper, the Cleveland Plain Dealer reported that O’Dell, the CEO of Diebold, is a major fundraiser of President Bush. Manjoo [Ma1] notes: ″In a letter to fellow Republicans, O’Dell said that he was “committed to helping Ohio deliver its electoral votes to the president next year.” Even the people involved in the aforementioned Project P1583 who had to design the new standard for electronic voting machines were not beyond suspicion. It was implied that the committee leadership is largely controlled by representatives of e-voting machine vendor companies and others with vested interests. The problem is that when counties, states or countries consider purchasing electronic voting machines they usually base their choice of machine solely on the information from the vendors [Ma3]. The opinion of unbiased technologists with no stakes in the voting system companies is often not taken into account and the decisions are made by people who don’t understand the issues and don’t understand much about how computer programs work.

3. Case Study: Security in the TruE-Vote system

The objective of the TruE-Vote project was to design and implement a secure Internet based voting system integrated with existing Public Key Infrastructures, and to demonstrate the possibilities of e-voting and e-polling by means of voting and polling experiments with Internet enabled users (members of community networks) and traditional users. The sociological analysis of the voting session results allowed us to understand the level of confidence and trust of the users in the technology, the relation between socio-cultural background and technological skills of the users and the level of acceptance of e-voting technology, and finally the effects of e-voting technology on voting behavior.

We conducted fourteen field studies in five different locations: in three local situations (Newham, a neighbourhood in London; Orsay, a small town in France; CGIL, the Milanese department of an Italian trade union) and in two community networks (RCM in Milan and OYK in rural Finland). Due to legal constraints, the system could not be tested in (national) elections. Nevertheless, in all test sites, two or three real voting events were organized by the local authorities or the trade union board about policy issues. For our study, we combined several methods and tools like questionnaires, direct observation, log files, analyses of the ballots and interviews with voters and ballot organizers. This paper uses the data from the internet enabled users at RCM and OYK.

During the design phase of the TruE-Vote system the project team had many discussions about the verifiability of the vote. Although at the time we did not know of any other electronic voting systems that provided a VVAT, we decided that to gain the trust of the users it would be wise to implement this requirement into the new system. Unfortunately, due to delays that are so common in large-scale projects, the technicians were not able to realize the VVAT in time for the pilots. The only form of verifiability provided took place within the system itself. The voter ticks the box of his choice, but

the vote is not actually cast until it is confirmed. When 'Confirm' is selected, the system will display all the operations required to actually cast the vote. Since verification takes place in the black box of the system, the users have no way of telling whether their votes were really cast the way they wanted them to be cast. The only thing that the system provides is a screen which offers a digital representation of the vote. The TruE-Vote system then asks the voter to confirm the choice they have made. However, you cannot see your vote actually being recorded. As Harris puts it: "Asking you to 'verify' your vote by saying yes to a computer screen is exactly the same, in terms of data integrity, as asking you to tell an election official your vote, which she then asks you to repeat while never letting you see what she wrote down. That procedure is absurd and would be trusted by no one" [Ha]. So, in the end a paper trail was not offered by the system. However, the questionnaires that were to be distributed among the participants were already designed based on the idea that the system would have a voter-verifiable paper trail. Since the field studies took place in different countries, the English questionnaires had to be translated into Finnish, French and Italian. Time constraints made it impossible to change them at the last moment and therefore the respondents were asked to respond to three statements about the verifiability of the system: 1) I could easily check that my vote has been counted 2) It is difficult to verify the vote 3) It is quick to verify the vote. The answers were measured on a six-point scale.

We were amazed to find that the majority of the respondents agreed mildly to strongly that it was easy for them to check that their votes had been counted (61 percent), while in fact the system does not provide this functionality. Only 5.8 percent disagreed strongly with this statement. The other two statements about the verifiability of the system showed similar results. 68 percent of the respondents disagreed mildly to strongly with the statement that it was difficult to verify their vote. In other words, they found it easy to verify their vote. Only 5.2 percent agreed strongly that it was difficult to verify their vote. Finally, in answer to the question whether it was quick to verify the vote 68 percent of the respondents said yes, and only 4.9 percent disagreed strongly. The next step was to test for correlations between a constructed variable named the 'verifiability' variable, in which we combined the three verifiability questions. We created this new variable by taking the mean of the scores on the three items. This variable measures the perceived level of verifiability of the TruE-Vote system. The neutral value is 3,5 with 1 as very much trust in verifiability and 6 as and no trust at all, respectively. The average is 2.9, indicating a moderate trust. We were surprised that the respondents were positive about the possibility to verify their vote and wanted to find out whether this opinion is related to personal characteristics (gender, age, computer literacy, opinion about usability of TrueVote and about ICT in general) or to context variables (place of voting, country).

We found that there is no relation between the *place of voting* and the users' opinion on the verifiability of the system. Whether respondents voted from home, work, school or a kiosk, they all gave similar answers to the three questions about the count of the vote. All of them were equally positive about the ease and speed of the verifying procedure. On the other hand, the *country* matters: we found that the respondents from Italy have a lower trust in the verifiability of the system than the Finnish respondents.

The level of *computer skills and experience* does not correlate with the opinion on the verifiability of the TruE-Vote system. We find this very surprising, as we expected that frequent computer users would have been far more critical about the security and verifiability of the system. We also expected that users with little computer experience would think that the system is verifiable, as they lack the knowledge which makes them understand what really happened. However, people who use the computer and the internet more frequent seem to judge the verifiability of the system in the same way as people who use the computer less. Also, users who judged themselves to be very expert with computers had the same opinion as people who saw themselves as hardly computer savvy. We did not find any correlation with the age of the respondents.

Women seemed to agree slightly more with the statements than the men, but the differences weren't very large. This corresponds with women's overall higher trust in the security of the system. From previous analysis of our data we found that the users hardly *trust the privacy* of the system, but do have reasonable *trust in the security* [OV]. What this means is that the respondents do not really fear fraud or attacks from hackers, but they are concerned about their personal data. When people signed up for the field experiments, they had to provide a large amount of personalized data to be put on the smart cards for identification purposes. From their answers to the questionnaires and from the e-mails they have sent us, it became clear that they worried that their personal data would be used for other purposes, or that their data would be linked to their vote. Women seemed to have a slightly higher trust in both the security and the privacy protection of the systems than men did. Users with a low trust in the security of True-Vote are also more concerned about the verifiability of the voting system than the people who do trust the security. This is what you would expect. We find the same for *trust in new technology in general*. People with a lower trust in new technologies believe less in the verifiability of electronic ballots. On the other hand, trust in privacy does not correlate with verifiability. Users who feel that new *ICT's can not be avoided* in the future have more trust in the verifiability of the system. Finally, there is a relation between the opinion about the usability and the opinion about verifiability (r = 0.545). People who find the TruE-Vote system easy to use (fast, easy to install, easy to connect, easy to correct mistakes, etc) also trust the verifiability more than people who rated the usability more negatively.

verifiability	**Mean (ANOVA)**	**Sign**	**N**
men / women	3.05 / 2,71	0.034	188 / 88
Italy / Finland	3.03 / 2.77	0.09	177 / 99
verifiability by	**Correlation (r)**	**Sign**	**N**
trust in security	0.32	0.000	272
trust in new voting technology	0.18	0.003	273
voting is public duty	0.12	0.048	273
unconcerned about privacy	0.13	0.034	272
unavoidability of ICT	0.24	0.000	274
usability	0.55	0.000	276

Table 1: Trust in verifiability by other variables

Summing up, we can say that the less concerned people are about the security of ICT in general, and the more they believe that the TruE-Vote system is secure, the more they also believe that the TruE-Vote system is verifiable. The same holds for the belief that new voting technologies indicate progress, the opinion that increasing use of ICT is

unavoidable, and the opinion about the general usability of the TruE-Vote system. Finally, the opinion about voting in general has some effect: the stronger one finds voting a public duty, the better one evaluates the verifiability of the system. So what do we learn from these findings? We have a system that does not show people that their votes are properly counted. Everything happens within the machine and is not visible for the users, but this does not seem to bother them too much. What is it that they actually trust? Is it the system? Or is it the authority of the organizers? The majority of the respondents say that they could easily check that their vote was counted. They said it was easy and quick to do this. Thus, their opinion is more based on *perception* than on facts. Does this mean that it is not important how secure a system is, as long as people trust it to be secure? Does this mean that as long as we tell the users a bunch of lies about the security, privacy or verifiability of the system they will believe it and act accordingly?

Our data show that the trust of users in relation to the verifiability of a system is not only related to the system itself, but also to things that have nothing to do with the technology. On the technology side of the system we saw that the trust in the security and the usability of the system plays a large role. People do base part of their opinion on these issues. The more people trust in the security and the better the usability of the system, the less they will doubt about the ability to verify the count of the vote. From this we learn that improving the security and the usability will have an impact on gaining or restoring public confidence and trust in e-voting systems. However, a lot of the variables that correlate with the trust in verifiability have nothing to do with the technology itself, but more with the social context in which the new technology is embedded. We saw that both the location and the gender of the participants play a role. Also trust in new technologies and the unavoidability of ICT's influences user's opinion. Users with a positive view on technology are more inclined to believe that the system is verifiable, even if this is not the case. We have seen in this paper that people will use insecure systems or black box technologies if they think of them as being secure. But how do people form their opinion about the security and privacy of new technologies and existing ICT's? Further research is needed to investigate which non-technical factors influence trust and the acceptance of new technology. First of all, we think that the reputation and professionalism of the organizing institution might have be a factor that influences the perception of people. If a local or national government is fully trusted by citizens then they are more likely to also trust the security of the system. This might explain the differences in opinion we saw between the Finnish and Italian respondents. Secondly, we think that the attitude of the mass media influences the opinion of the users. When newspapers or TV programs cover negative stories about certain technologies (rightfully or not), people will be influenced by this accordingly. Thirdly, the views of friends, family and colleagues may play an important part in forming an opinion. Finally, one could assume that the convenience that a new technology might bring people will influence their opinion about it. We will take the mobile phone as an example of this argument. Ever since people started using mobile phones the issue of electromagnetic field radiation from cell phones has been controversial. Most experts believe that it is insignificant. However, there is a significant body of evidence to suggest that cell phone radiation can indeed cause health problems [HH; Re]. The debate about the risk of mobile phones for the health of the users is still ongoing and users

receive mixed information about the risks of mobile phones. Nonetheless, the majority of people decided to trust the safety of the phones and use them despite the concerns because they bring them so much convenience. From this it is obvious that users of technology pay more attention to first-order effects than to second-order effects. Therefore it is likely that if citizens see e-voting as a convenient way to cast their votes, they might be less concerned about its security issues. This could also work the other way around. A system could be one hundred percent safe and secure, but if users don't trust it they will not use it.

4. Conclusions

With current voting systems, errors are likely to be on a relative small scale. Electronic voting, on the other hand, substantially increases the scale of potential problems. This has its impact on public confidence. The complex technical questions with regard to security and other issues of e-voting systems should be answered before the systems are to be used at governmental elections on any level. At the moment the topic of voter-verifiability is very much in the limelight. In order to guarantee a true democracy it is important to have as secure a voting system as possible. Requiring a VVAT is, as we have seen, one important step in that direction.

Many technologists think that the solutions for security and trust issues lie in adjusting and improving the technology. Dill says: "Instead of trying to convince people the machines are safe, the industry should fix the technology and restore public confidence by making the voting process transparent, improving certification standards for the equipment and (ensuring) there is some way to do a recount if there is a question about an election" [Ze]. But is this the best solution? Will users trust the system more when it is more secure? Will offering voter-verifiable paper trails work to gain trust from people or are there other non-technological issues that are of equal or more importance? Some well-known technologists like Diffie, Zimmermann, Stephenson, all known for their work on cryptography and Berners-Lee, creator of the World Wide Web, start to acknowledge the limitations of a techno centric approach to the complicated questions of privacy, security and freedom. They are moving towards recognition of social and political realities. True techno-believers are sure that they can guarantee the privacy and security of people with physics and mathematics. But after thirty years of working on perfecting cryptography some of the techno-believers are changing their views on privacy and security issues and admit that you have to trust 'social structures'. It is a rejection of the ideal of trust in physics and mathematics [Ul].

From our research within the TruE-Vote project we have indeed seen how important the social context is for the trust people have in a system. People should not just have to trust in the integrity of a voting system or the people who designed, developed and implemented it. With a system so crucial to the existence of our democracy trust in technology alone is not sufficient. In order to fully understand citizens' willingness to use electronic voting systems we need to look as much into the sociopolitical issues as into the technological issues. Both need to be taken into account to make electronic voting a secure and successful new voting method.

5. Acknowledgements

The TruE-Vote project (IST-2000-29424) was partly funded by the European Commission. We are grateful to our partners: Postecom, CGIL, Abacus, RCM, Smile, and the University of Milano (all Italy), Certinomis, Orsay (both France), Glocal (Finland), Newham (UK), NIWI-KNAW (Netherlands). Part of the work was done in the former Social Informatics group at the University of Amsterdam. We would like to thank Vanessa Dirksen and Bruce Clark for their comments.

References

[Co] Coleman, S. et al. (2002) Elections in the 21st century: from paper ballot to e-voting. The Independent Commission on Alternative Voting Methods. London: Electoral Reform Soc.

[CC] Collier, J., Collier, K. (1992) VoteScam: The Stealing of America. Victoria House Press.

[Di] Diebold Election Systems (2003) Checks and Balances in elections equipment and procedures prevent alleged fraud scenarios.

[HH] Hardell, L., Hallquist, A., Hansson, K., Mild, K.H., Carlberg, M., Phlson, A., Lilja, A. (2002) Cellular and cordless telephones and the risk for brain tumours. European Journal of Cancer Prevention v.11, n.4, Aug02.

[Ha] Harris, B. (2003) Black Box Voting: Vote Tampering in the 21st Century. Elon House/Plan Nine.

[IPI] Internet Policy Institute (2001) Report of the National Workshop on Internet Voting: Issues and Research Agenda.

[KS] Kohno, T., Stubbefield, A. Rubin, A., Wallach, D. (2003) Analysis of an Electronic Voting System. Johns Hopkins Information Security Institute technical Report TR-2003-19.

[Ko] Konrad, R. (2003) E-voting critics point to security hole. California primary results appeared online before polls closed. Associated Press MSNBC News.
Online: http://stacks.msnbc.com/news/964736.asp?0dm=n15ot

[La] Landes, L. (2002) Elections in America – Assume Crooks Are In Control.
Online: http://www.commondreams.org/views02/0916-04.htm

[Ma1] Manjoo, F. (2003) Hacking democracy?
Online: http://www.salon.com/tech/feature/2003/02/20/voting_machines/print.html

[Ma2] Manjoo, F. (2003b) Another case of electronic vote-tampering?
Online: http://www.salon.com/tech/feature/2003/09/29/voting_machine_standards

[Ma3] Manjoo, F. (2003c) An open invitation to election fraud. Online:
http://www.salon.com/tech/feature/2003/09/23/bev_harris

[McG] McGaley, M., Gibson, J.P. (2003) Electronic Voting: A Safety Critical System.

[Me] Mercuri, R. (2001) Dr. Rebecca Mercuri's Statement on Electronic Voting.
Online: http://www.notablesoftware.com/RMstatement.html

[OV] Oostveen, A., Van den Besselaar (2004) E-democracy, Trust and Social Identity: Experiments with E-voting technologies. Forthcoming.

[Re] Rense, J. (2002) Some Early Cellphones Pose Increased Brain Tumor Risk.
Online: http://www.rense.com/general28/cisire.htm

[SV] Sequoia Voting Systems (2003) Sequoia Discusses Safeguards of Electronic Voting.
Online: http://www.sequoiavote.com/article.php?id=50

[Ul] Ullman, E. (2000) Twilight of the crypto-geeks.
Online: http://www.salon.com/tech/feature/2000/04/13/libertarians

[Ze] Zetter, K. (2003) E-Vote Firms Seek Voter Approval . Wired News.
Online: http://www.wired.com/news/evote/0,2645,60864,00.html

Towards remote e-voting: Estonian case

Epp Maaten

Elections Department
Chancellery of the Riigikogu (Parliament)
Lossi pl. 1A
15181 Tallinn, ESTONIA
epp.maaten@riigikogu.ee

Abstract: This paper gives an overview about the Estonian e-voting system. Paper discusses how the concept of e-voting system is designed to resist some of the main challenges of remote e-voting: secure voters authentication, assurance of privacy of voters, giving the possibility of re-vote, and how an e-voting system can be made comprehensible to build the public trust.

1 Introduction

The possibilities of implementing e-voting have been actively discussed in Estonia already since 2001. In 2002 the legislative basis to conduct e-voting was created. In summer 2003 by the National Electoral Committee the e-voting project was initiated.

The e-voting project serves the Estonian government's goal of using digital technology to help making the public sector more efficient, effective, and customer-friendly. The coalition agreement of the current government states that e-voting should be available starting from local government council elections of 2005 and for the following elections.

A number of countries use electronic voting machines within polling stations to e-enable elections, but this has not been an option for Estonia. E-voting in the context of Estonia means remote voting via Internet. The main goal is to provide voters an extra opportunity to cast their vote and thereby increasing voter participation.

2 Legislative basis

According to Estonian election legislation[1] e-voting takes place during the advance voting period from 6th to 4th day before Election Day. The following requirements of e-voting are laid out:

"(1) On advance polling days, voters holding a certificate for giving a digital signature may vote electronically on the web page of the National Electoral Committee. A voter shall vote himself or herself.

(2) A voter shall identify himself or herself by giving a digital signature.

(3) After identification of the voter, the consolidated list of candidates in the electoral district of the residence of the voter shall be displayed to the voter on the web page. The opportunity for the voter to examine the national lists of candidates shall be provided.

(4) The voter shall indicate on the web page the candidate in the electoral district of his or her residence for whom he or she wishes to vote and shall confirm the vote.

(5) A notice that the vote has been taken into account shall be displayed to the voter on the web page."

E-voting shall be an additional voting option. The other options existing today, which are voting at the polling place or by embassies, advance voting outside of polling place of voter's residence and voting by mail in foreign states, remain.

3 Basic principles of e-voting

The main principle of e-voting is, that it must be as similar to regular voting as possible and compliant with election legislation and principles. E-voting should offer the same level of security and confidence as traditional voting. Therefore according to the electoral laws e-voting must be uniform and secret, only eligible persons must be allowed to vote, every voter should be able to cast only one vote, a voter must not be able to prove in favour of whom he/she voted. At last, the collecting of votes must be secure, reliable and accountable.

From a technical point of view the e-voting system must be as simple as possible as well as transparent so that a wide range of specialists would be able to audit it. The e-voting system must be reusable in a way that developing a new system for the next voting is not needed.

---

[1] Riigikogu Election Act, Local Government Council Election Act, Referendum Act and European Parliament Election Act – all 4 election acts contain similar terms for e-voting.

The following principles are specific to Estonian e-voting concept:

* ID-cards are used for voter identification;
* Possibility of electronic re-vote – e-voter can cast his/her vote again and the previous vote will be deleted;
* The priority of traditional voting – should the voter go to polling station on voting day and cast a vote, his or her e-vote shall be deleted.

3.1 Voters authentication with ID-card

Estonia has implemented ID card as the compulsory document for identifying citizens and alien residents living within the country. The card, besides being a physical identification document, has advanced electronic functions that facilitate secure authentication and legally binding digital signature, in connection with nationwide online services. ID-cards are equipped with a chip containing electronic data, certificates and their associated private keys protected with PIN-codes. The ID card functions as an electronic identity, enabling to use services online conveniently and securely.

According to law a voter identifies himself or herself by giving a digital signature. This is a crucial point laid down by law to avoid security risks related to voter identification during remote e-voting. The introduction and rapid spread of ID-cards provides the necessary tools for e-voting – electronic voter authentication and possibility to give digital signatures.

The use of ID-card is a different approach to solve the problem of voters identification. In some countries, which are piloting the e-voting, identification codes are sent to the voters often by post. It would be quite insecure method for Estonia. For different reasons many citizens have not been interested to disclose their real home address to the national population register. Because of incorrect information of the register many envelopes with codes necessary for identification would be lost or would reach a wrong addressee.

Widespread use of ID-card is vital – in regards to Estonian e-voting, systems that require previous on-the-spot registration are not considered. Recently a number of mass-market projects using the ID-card were started. For instance in the public transportation system of the capital city of Tallinn a new virtual ID-card-based payment and control system is employed. Residents, willing to use the Tallinn public transport!and other services for city residents at discounted prices, have to obtain an ID-card.

The number of ID-card holders has increased very rapidly during the last year. By now about 500 000 ID-card have been issued[2]. By the 2005 elections this number should approach 800, 000, meaning that most of the eligible voters (about 1 Million for local elections) should be covered [GD04; P 4].

3.2 Electronic re-vote and the priority of traditional voting

In the concept of e-voting two principles are important:

---

[2] Statistics of issuing the ID-cards: : http://www.id.ee/pages.php/03020504

* *The possibility of re-vote* – voter has a chance to cast his/her vote again; Voter is allowed to vote electronically more than once. In this case the previous e-vote will be deleted. Multiple voting is mostly considered as a crime, but according to General Description of the E-Voting System only one e-vote per voter, the last one will be entered into the electronic ballot box [GD04; P 7]. Electronic re-vote cannot thus be considered as multiple voting, as the system will take into account only one vote.Allowing to re-vote is considered as a measure against vote-buying and against voting under coercion. Remote voting in an uncontrolled area can be easily manipulated. A voter could be coerced into voting for a particular candidate or voters have the opportunity to sell their vote. By re-voting the voter who was illegitimately influenced can cast a new vote once the influence is gone.

* *The priority of traditional voting* – if the voter goes to polling station on Election Day before 16.00 and casts the vote using a paper ballot, then his or her e-vote cast during advance voting period, will be deleted.

The justification of this principle is similar to the previous one. The principle makes also possible to declare the e-voting invalid in the case the e-voting system used during advance polls has been seriously compromised or rendered. Then the voters still have the possibility to participate on elections and vote traditionally on Election Day.

4 General concept of e-voting - the envelope method

It is highly important that public confidence in the election process remains strong. The right of individuals to vote is one of the main principles of democracy. Great effort and care should be taken to ensure that elections as well as e-voting, which is a part of whole election process, are conducted in a fair manner. A research about public opinion concerning e-voting shows that people mostly trust electronic services available through Internet (banking, for instance) and thus they also tend to trust e-voting. On the other hand there is a lack of information what e-voting actually means and many people could not answer the question about trusting the system [RCF04; P 22, 23]. As the detailed e-voting concept has been published only in January 2004, it has not been widely discussed by media.

It is important that e-voting could be explained as simply as possible to be understandable for voters. One way to simplify the complexity of e-voting is to draw parallels to ordinary voting. The e-voting scheme is similar to the envelope method used during advance polls today:

* the voter identifies himself/herself to polling commission,
* the voter fills the ballot and puts it in an inner envelope,
* that envelope is put into another envelope on which the voter's data is then written,
* the envelope is transported to the voter's polling station, the voter's eligibility is verified, and if the voter is eligible, the outer envelope is opened and the anonymous inner envelope is put into the ballot box.

The e-voting follows the same scheme:

* The voter inserts the ID-card into a card reader and opens the homepage of the National Electoral Committee,
* a relevant candidate list of voter's constituency is displayed according to the voters personal identification number,
* the voter makes his/her voting decision, which is encrypted and can be defined as inner envelope,
* the voter confirms his/her choice with a digital signature and the outer envelope comes up, voter gets a confirmation, that his/her vote has been recorded,
* at the vote count the voter's digital signature (outer envelope) is removed and at the final stage the members of the National Electoral Committee can only collegially open the anonymous e-votes and count them.

The following figure illustrates the envelope method:

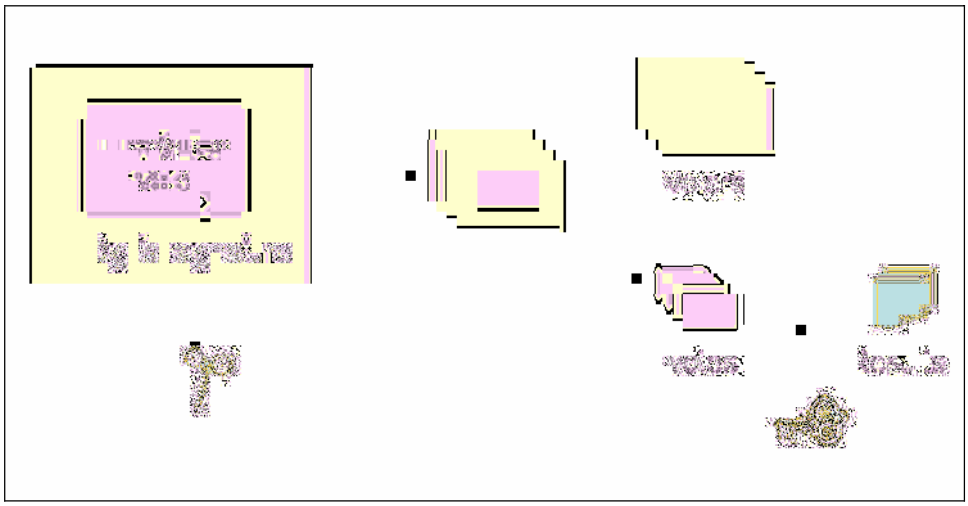


Fig 1: The envelope method [GD04; P 9]

Public-key cryptography is used here. Application encrypts voter's choice with the system's public key and voter confirms the choice by signing it digitally. The votes are collected, sorted, voter's eligibility is verified and double votes are removed. Then the outer envelopes (digital signatures) are separated from inner envelopes (encrypted votes).

Inner envelopes are forwarded to the National Electoral Committee who has the private key of the system. Voter's choice encrypted with the system's public key can be decrypted only with private key. To ensure the voter's privacy the requirement is, that at no point should any part of the system be in possession of both the digitally signed e-vote and the private key of the system. In order to count e-votes, the system's private key is activated by key-managers according to the established key management procedures. The counting of votes takes place in the vote counting application, separated from the network.

The lists of voters who voted electronically are compiled from outer envelopes - from voter's ID-numbers. These lists are sent to local polling stations and on Election Day it is easily detectable if a voter who has already voted electronically, comes to polling station to vote by paper ballot. In that case the polling station committee informs the National Electoral Committee and voter's e-vote shall be deleted.

There are always two participating parties in voting – the voter and the vote receiver. The weakest link of the e-voting procedure is probably the voter's personal computer as no control can be exerted over it. The central servers which are under National Electoral Committee's responsibility can be controlled, however the errors and attacks, which may occur there influence a large amount of votes simultaneously. The e-voting system should take these issues very seriously.

The following considerations speak in favour of the envelope method:
* simplicity and clearness of the scheme, possibility to draw a parallel with traditional elections;
* simplicity of the system architecture – the number of components and parties is minimal;
* full use of digital signature.

The e-voting system shortly described here enables a basis for conducting e-voting at least as securely as traditional voting upon condition that that sufficient organisational, physical and technical security measures are implemented.

These were the main principles of the selected envelope system. Obviously the scheme is more complex in reality, offering additionally a possibility to securely cancel e-votes, covering detailed architectural components of the system, different organisational parties etc.

5 Problems decelerating the implementation of e-voting

There are many aspects of elections besides technical security problems that may bring e-voting into question.

E-voting brings along many concerns of fraud and privacy associated with remote balloting, including the risk that voters who do not cast their votes in the privacy of a voting booth, may be subject to coercion, or that voters have the opportunity to easily sell their vote. During the last elections in Estonia some vote-buying incidents became public and the problem has been blown up in mass media. This is partly the reason why the e-voting concept suggests that the re-voting should be allowed. The fact that voter has always a possibility to re-vote, even in the controlled area on elections day, can minimise the number of manipulative attempts.

The legislative basis to conduct e-voting has been created but according to e-voting concept evolved during the last year, the election laws should be amended in some crucial points like allowing to re-vote electronically. Also the priority of traditional voting should be enacted. It is indispensable to convince politicians that the e-voting system can still guarantee that there is only one vote per voter in the ballot box.

The number of people holding **ID-cards** has increased very rapidly but possessing the card is not enough for e-voting. Giving a digital signature implies that voter had a computer with the proper software installed and a card reader. The software enabling the use of the ID-card and digital signature is freeware, the card reader costs about 20 €. Thus, insufficient number of card readers, the complexity of software installation and the lack of knowledge how to give a digital signature may endure as obstacles of widespread e-voting.

Privacy is a key issue in e-voting. Like in most European countries, also in Estonia voting privacy in ordinary voting is guaranteed by forcing voters to vote alone in a voting booth. Voting in an uncontrolled area means, that there is no guarantee for privacy any more. However, it is not solely a problem of e-voting. Similar concerns arise if voting by mail is allowed. This aspect cannot be ignored, but as the possibility of traditional voting remains, voters who are worried about the privacy can choose the paper balloting.

A mention must be made of the **sociological problems**. Remote voting also requires technology and the knowledge to use it. If remote voting were to become the dominant form of voting, it could result in an increased digital divide caused by Internet access and computer skill barriers. Even if e-voting is an additional voting option, the proportions between voter's age groups may change. In 2002 the share of Internet users was 39% in the 15-74 age bracket, but the percentage is much higher among the young people [DD02]. It is reasonable to assume that e-voting will activate people, who would not participate in voting at polling stations.

Some steps towards overcoming the **digital divide** are already made. Since 2001 a national training project during which about 10% of the adult population of Estonia received free elementary computer and Internet training, has been carried out [LW04, P 2]. To improve the Internet access another project named "Village Road" was launched. The aim of that project is to establish Internet connection in Estonian public libraries, to establish of Public Internet access points in them, and provide with workplace computers and software. In 2003 all access points have been supplied with smart card readers so that people would be able to use e-services with their ID-card. In April 2004 about 550 access points existed [LW04, P 12].

There are still many concerns about the **confidentiality** of electronic voting and fears that a vote can be related to voter. An information campaign could be one of the measures to make the details of e-voting security, including the role of cryptology in it, publicly acquainted. Building public trust is one of the most difficult aspects of introducing the e-voting. The proposed e-voting methods need public acceptance otherwise legitimacy of e-voting can be placed in doubt.

6 Current state of e-voting project and future plans

During the last year a technical and organisational concept of e-voting has been prepared, which in turn has been subjected to a thorough security analysis. Afterwards the technical planning of the system has been made. A public procurement procedure was carried out and the contract to develop the e-voting software was given to the Estonian company named Cybernetica Ltd. The software should be ready by autumn 2004 and further it will be a subject to audit. The key management and audit regulations are under work.

In late 2004 the first pilot project is planned, where the whole e-voting system will be put to test. This pilot will, according to current plans, take place in the capital city of Tallinn in a form of consultative referendum. After the test and the audit further plans can be made. As mentioned before, the next pilot is planned for the local government council elections in October 2005.

It is not clear if e-voting could raise the level of voter turn-out. However, it is a measure, which may hinder the steady decrease of turn-out percentage. Remote e-voting is regarded as an added value to the voter and a measure of widening of the democracy. Growth of online interaction and presence can be witnessed by the exponential increase in the number of people with home computers and Internet access. Since the idea of e-voting became public in 2001, many people in Estonia expect that e-voting becomes an integral part of today's information society as soon as possible. There are strong views that rapid developments of information society should be taken into account in state's democratic practice.

A step-by-step approach when introducing e-voting is regarded as absolutely necessary: from testing to piloting, from small to bigger numbers of potential voters, from restricted to general elections. For Estonia there is a long way to go towards the successful implementation of remote e-voting, but at least we have started off and took the first steps on this way. We try to make our best that this way will bring success.

Literature used

[GD04] The Estonian National Electoral Committee: General Description of the E-Voting System, Tallinn 2004. http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

[RCF04] Research Centre Faktum: E-voting and decrease of alienation. Tallinn, January 2004. P 23-27. http://www.parlament.ee/?id=846

[DD02] M.Kalkun, T.Kalvet , Emor and Praxis Centre of Policy Studies: Digital Divide in Estonia and How to bridge it, Tallinn 2002, P 49.

[LW04] Look@World Foundation: Internet Training Project Report, Tallinn 2002, P 2. http://www.vaatamaailma.ee/pls/VM/docs/FOLDER/VAATA_MAAILMA2/DOKUMENDID/PROJEKTID/LW_TRAINING_PROJECT_REPORT.PDF

Experimentation on Secure Internet Voting in Spain

Andreu Riera, Gerard Cervelló

Scytl Online World Security, S.A.
Entença, 95, 4-1
08015 Barcelona, SPAIN
andreu.riera@scytl.com
gerard.cervello@scytl.com

Abstract: A major step forward along the path towards the implementation of secure Internet voting in Spain was taken in November 2003. For the first time in this country, a non-binding remote electronic voting pilot was run in parallel to a public election, in particular the 2003 election to the Parliament of Catalonia. The e-voting pilot was also the first of this kind to gain the requisite approval by Spain's Central Electoral Council, ant it is still the most significant up to date. The objective of the trial was to evaluate the advantages, usability, security and reliability of this voting system in consideration of its potential use in future elections, mainly as a complementary channel to postal voting. The trial provided valuable empirical information regarding practical technological and social issues surrounding e-voting.

1 Introduction

Since 1996 the *Generalitat de Catalunya* (the government of the autonomous region of Catalonia located in the north-east of Spain) had run several pilots in parallel to public elections using electronic voting machines in polling stations [Aa99]. Following the interest in the development of Internet voting throughout Europe, the *Generalitat de Catalunya* organized its own non-binding remote electronic voting pilot that was run in parallel to the 2003 Elections to the Parliament of Catalonia [GC03]. This was the first time a *remote electronic voting* pilot run in parallel to actual public elections in Spain received approval by the Spanish *Central Election Council*[1].

The Generalitat wanted to evaluate the advantages, usability, security and reliability of this voting system in consideration of its potential use in future elections which would be mainly as a complementary channel to postal voting. For this reason, over 23.000 Catalans resident in Argentina, Belgium, the United States, Mexico and Chile were invited to participate using any computer connected to the Internet by means of a web browser supporting Java technology.

---

[1] The Spanish Central Election Council has been always very reluctant to this kind of e-voting pilots run in parallel to current elections.

The pilot was managed by the *Oficina de Coordinació Electoral de la Conselleria de Governació i Relacions Institucionals* of the *Generalitat de Catalunya*, and used Pnyx, the cryptographic technology for securing electronic voting developed by Scytl [SCT03].

In this paper, we present the Catalan remote e-voting experience along with our views with regard to the security standards that must be set in electoral processes driven by electronic voting systems, implemented in this pilot. In Section 2 we start by providing the objectives drafted by the Generalitat to judge the success of the pilot. In Section 3 we introduce briefly the currently most debated risks and challenges posed by electronic voting, along with the solution offered by Scytl's security architecture. In Section 4 we present an overview of the e-voting pilot phases. Section 5 shows the results of the e-voting pilot in comparison with the results from the real elections. Section 6 introduces the feedback provided by the users of the e-voting platform, and finally, Section 7 includes some concluding remarks.

2 Pilot Objectives

The Catalan Government set some specific objectives that were used to judge the success of the pilot. In this respect, the remote internet voting system had to:

- **Facilitate the participation of voters that are resident abroad.** At present these voters can only vote by mail, and many of them do not receive their ballot or have problems sending it back on time for it to be counted.
- **Guarantee the honesty of the electoral process**. The system must offer at least the same level of security and confidence found in traditional paper-based postal voting.
- **Facilitate participation in the election**. The installation of any specific software or hardware should not be required.
- **Extend the polling period without increasing the man-hours required to staff the election**. The current postal voting system entails a logistical challenge that new technologies can simplify and make less expensive.
- **Protect the voter's personal data from third parties.** This security measure is essential to ensure compliance with the Spanish Law of Personal Data Protection.
- **Obtain the results immediately after the polls close**. This permits the integration of the results from the remote voting with the results from the polling-place voting without having to wait several days for the postal votes to arrive.

3 Description of the Pilot

The *Generalitat de Catalunya* selected *Pnyx*, the e-voting security technology from Scytl Online World Security S.A. to run the project. The project was managed by the *Oficina de Coordinació Electoral de la Conselleria de Governació i Relacions Institucionals de la Generalitat de Catalunya*.

The non-binding pilot was run in parallel to the 2003 Elections to the Parliament of Catalonia, held on November 16th 2003. 23.234 Catalans in Argentina, Belgium, United States, Mexico and Chile were invited to try the internet voting system from 10h00 on November 14th until 20h00 on November 16th. Voters could participate from any computer connected to the Internet using any web browser supporting Java, a technology required to cryptographically process every individual ballot to ensure its security. In addition, several "Casals Catalans" (Catalan cultural associations spread all over the world) allowed voters to use computers located in their offices overseas.

3.1 Creation and Distribution of the Voting Credentials

To cast a vote during the e-voting pilot, each voter had to be correctly identified in order to ensure his/her presence in the electoral roll and that he/she had cast no previous ballot. After evaluating several alternatives, the login/password option was selected, due to its usability and easy distribution, as the mechanism for accessing the e-voting platform.

For security reasons, the process for the creation and distribution of voting credentials ensured that no entity had access to both the voting credentials and the personal data of the voters. A 16 character voter identification key was randomly generated for each participant. This information was sent to a printing company that printed the keys in sealed PIN envelopes. A different company was responsible for the task of enclosing the sealed PIN envelopes, an invitation letter from the Generalitat, and some brief instructions into a larger envelope that was addressed and sent to each voter by surface mail 15 days before the pilot was to begin. This credential distribution process is identical to the one used to allow all Spanish citizens living abroad participate in the paper-based elections: they receive by mail all the ballots, and then they send their selection again by mail to the Spanish electoral authority before a deadline.

3.2 Pilot Promotion Campaign

The pilot did not have an extensive promotion campaign. Besides the letter sent to each voter, a brochure was sent to the Spanish Consulates and Casals Catalans in the countries involved. A website [GC03] was set up where the participants could access to information about the pilot and an e-mail address (gencat@e-lectoral.com) was created where questions regarding the pilot could be sent that would be responded to by Scytl technical personnel.

3.3 Constitution of the Electoral Board

The e-voting platform used in the pilot was designed to replicate the essential trusted security features of a traditional election [Ra03]. One important aspect of such elections is the oversight of an electoral board that is composed of several members who may have opposing interests in the election results. The e-voting platform empowers an electoral board whose role is to control the election electronically.

On November 13th at 18h00 a representative of each political party represented in the Parliament of Catalonia (5 parties in total), along with the director of the Oficina de Coordinació Electoral and a representative of Catalan Government assembled together to constitute an electoral board to manage the pilot. Following a short simple procedure, a cryptographic key that protects the confidentiality of the votes and that is necessary to start the tallying process, was generated and divided in 7 parts, one for each member of the electoral board. Immediately after, it was destroyed.

3.4 Vote Casting Procedure

Scytl's Pnyx-based electronic voting platform permits voting from any Internet-connected computer, running a browser that supports Java (virtually 100% of the browsers on the market). Java is needed to guarantee the security and confidence requirements of the Internet voting platform. It is used to create a secure cryptographic dialogue between the voter and the electoral board, ensuring that the vote is encrypted at the voter's browser and remains so until it is delivered to the electoral board. The Java applet that is downloaded onto the voter's browser is digitally signed for authentication and integrity purposes.

To cast their votes the participants had to follow a simple identification procedure on the voting website, using the credentials that had been sent to them by post, as explained before. Once correctly identified, the voter selected one candidate list from the selection presented on-screen (including the blank vote option), and then clicked on a button to cast the ballot. Before casting the ballot, the Java applet presented another screen to confirm the choice done by the voter, and, once confirmed, the vote underwent a series of cryptographic operations in the Java applet to encrypt the vote, which was sent over the Internet to the voting server. This series of operations lasted on average a couple of seconds.

Once the vote was sent and confirmed, the applet provided a voting receipt that enabled the verification of the vote's inclusion in the final tally. The voting receipt consisted of a unique vote identifier (the vote's serial number) and the control code (actually the digital signature of the vote identifier and other election data).

The Java applet controlled all of the important operations in the voting process, so that voter's trust only needed to be placed in this audited and digitally signed piece of software and in the electoral board that oversees the process.

3.5 Vote Tally and Verification of Results

The vote tally was performed on November 16th in the World Trade Center of Barcelona, the same location where the real elections outcome was spread from, once the polls were closed at 20h00. The ballot box was opened and the tally initiated by the 7 members of the Electoral Board in front of more than 20 national and international observers as well as representatives of the Electronic Voting Study Group of the Spanish Senate. It took only 23 seconds to decrypt the votes and to obtain the results after the polls closed. The results and the voting receipts used for the result verification were published on November 17th on the official website of the pilot [GC03].

4 Electoral Results

Table 1 contains a list of the aggregated results of the pilot vote. No invalid votes were received (as it was expected) with 11 blank votes received, and 719 votes received for candidates for a total of 730 votes cast on the e-voting platform, which means a participation of 15.23% of the voters who cast a ballot by mail. These results were considered a success by the *Generalitat of Catalunya*.

Electoral Roll	Real Votes Received	Pilot Votes					
		Votes Received	Abstained	Invalid votes	Blank votes	Votes for Candidates	Valid Votes
23,234	4,794 (20.63%)	730 (3.14%)	22,504 (96.86%)	0 (0.00%)	11 (1.51%)	719 (98.49%)	730 (100.00%)

Table 1: Aggregated Results of the Pilot Vote

Table 2 compares participation rates of postal voting with those of Internet pilot.

Country	Electoral Roll	Method of Voting	Votes Received	Abstained	Participation Rate	Internet as a % of Postal
Total	23,234	Post	4,794	18,440	20.63%	**15.23%**
		Internet	730	22,504	3.14%	
Argentina	10,539	Post	3,034	7,505	28.79%	**9.56%**
		Internet	290	10,249	2.75%	
Belgium	1,876	Post	632	1,244	33.69%	**8.70%**
		Internet	55	1,821	2.93%	
USA	4,210	Post	409	3,801	9.71%	**38.63%**
		Internet	158	4,052	3.75%	
Mexico	4,528	Post	68	4,460	1.50%	**226.47%**
		Internet	154	4,374	3.40%	
Chile	2,081	Post	651	1,430	31.28%	**11.21%**
		Internet	73	2,008	3.51%	

Table 2: Comparison of Postal Votes to Internet Votes

The participation figures for the pilot highlight some interesting results. While over 15% of voters who voted by mail also participated in the pilot by voting a second time by Internet, there was a large variance in participation rates depending on which country the voter voted from. The lowest participation rate was 8.7% for Catalans living in Belgium while in Mexico it was 226.47%, meaning that more than twice as many people voted in the pilot than returned a postal vote in the real election. Over one third of the Catalans resident in the U.S. who voted in the election also participated in the pilot (38.63%).

There are probably at least two important factors affecting these rates: the level of Internet penetration in the country of residence, and the speed / reliability of the postal service in these countries. One might expect that the participation in the United States to be higher than that of Argentina due to the higher penetration and use of the Internet in North America. It has been suggested that the very low participation rate in Mexico was due to problems receiving the postal ballot in time to return it to Catalonia to be counted before the deadline. This latter case neatly highlights one of the biggest advantages of Internet voting, in that it enables higher participation rates, especially among those who experience difficulties voting by mail. Regarding the participation from the Casals Catalans, Scytl is only aware of about 40 people voting from three different ones located in Argentina and Mexico.

5 Voter Feedback

One of the electronic remote voting pilot's aims consisted in evaluating the opinions of the voters regarding this new voting method. After voting, voters were asked to fill in a simple survey located on the same voting website. From the 730 voters that participated in the pilot, 563 (over 77%) answered the survey, with 216 voters providing comments. Table 3 provides a summary of the survey responses.

Survey Questions	#Resp.	%	Survey Questions	#Resp.	%
1. In general, how would you describe the remote electronic voting pilot experience?					
Very satisfactory	397	70.52%	Satisfactory	151	26.82%
Unsatisfactory	10	1.78%	Very Unsatisfactory	5	0.89%
2. What confidence does the remote electronic voting process give you?					
Much confidence	286	50.80%	Reasonable	255	45.29%
A little confidence	18	3.20%	No confidence	4	0.71%
3. How would you rate the electronic and remote voting process?					
Very easy to use	347	61.63%	Easy to use	206	36.59%
Complicated	9	1.60%	Very Complicated	1	0.18%

4. What factors are most important to you when using a remote electronic voting platform like the one in the pilot? (Multiple answers are possible)					
Comfort	411	73.00%	Security	187	33.21%
Ease of use	146	25.93%	Others	15	2.66%
5. Would you have chosen this voting system if it had been a real (and binding) alternative to postal voting?					
Definitely	471	83.66%	Probably	82	14.56%
Unlikely	3	0.53%	Definitely not	4	0.71%

Table 3: Summary of Survey Results

The voter's opinions showed a clear approval of the system: over 97% were satisfied or very satisfied with the experience, 96% found that the system gave much or a reasonable amount of confidence, 98.2% considered that the voting process was easy or very easy to use, and 98.2% definitely or probably would have chosen this system to vote if the process would have been binding. Finally, of the factors that the voter considered as the most important in using the system, the comfort of easily voting from home is chosen (73%) as a big advantage of Internet voting, and the security offered by the system represents the next important thing to consider (33.2%).

6 Security risks and proposed solution

As broadly accepted, electronic voting and electronic consultation have the potential to improve our electoral processes and enhance democracy in many ways [HD00, Ch02, CM03, Ra02]. However, electronic voting is not problem-free. A whole new set of risks and challenges is created by this new voting scenario that is based on the use of electronic voting systems [MN03]. These risks and challenges can be broadly classified in three categories: legislative, socio-political and technological. An analysis of several socio-political and technical concerns can be found in [Ra02].

This section focuses on the currently most debated risks and challenges that relate to security, trustworthiness and confidence [Ra02, BM03, Jd04], proposing solutions to address them.

Traditional paper-based voting systems obtain their confidence through the direct, face-to-face interaction between voters and election authorities, as well as the physical evidence (paper ballots) that remains after the polling places close. Ballot secrecy and integrity is preserved by paper envelopes and physical ballot boxes. The fairness of the tallying process relies on the fact that electoral boards are composed of (and/or monitored by) people of opposing interests (e.g. members of different parties), which presumably prevents any collusion to alter the election results. Moreover, independent third parties and observers supervise the entire electoral process.

In contrast, pure electronic voting introduces a totally new interface between voters and election authorities and it removes the *physical* audit trails. The straight human-to-human interaction is substituted by a variety of hardware and software components, whose inner workings are not easily accessible or understandable. A new and complex technological infrastructure is interposed between the voters and the election authorities who in the end will tally the votes, obscuring the transparency of the ballot casting process. In addition, to create and administer this new infrastructure, technicians control the computer systems that are between the voters and the electoral board. Through their positions and functions, these technical people have many privileges that could be used to corrupt the electoral process. Therefore, naively implemented electronic voting systems can pose very serious threats to election integrity and shake the public's confidence in elections. Advanced security measures are clearly needed, to achieve the desired level of trust

We propose a security architecture for electronic voting that replicates the conventional security measures found in traditional elections. The principal objective of this architecture is to avoid putting all of one's trust on the computing infrastructure and on the technical people operating between the voters and the electoral authorities. The group of systems that compose the front-end of an electronic voting system (the systems that capture the ballots, e.g. web servers) are by definition complicated machines and difficult to completely protect or to certify, even more if connected to the Internet.

Our proposal consists in maintaining a clear separation of critical and non-critical modules. In this way we propose changing the current paradigm of electronic voting, in which the casting, recording and counting of ballots is grouped in a unitary, complex system, more easily accessed by technicians than by electoral board members. We propose to place all the critical tasks on two simple modules located at the extremes of the system (the voter and the electoral board). By means of end-to-end, application-level cryptographic protocols designed specifically to address the problems associated to electronic voting, a direct secured voting dialog can occur between the voter and the corresponding electoral board. The integrity of the electoral process is no longer exposed to the rest of the electronic voting infrastructure, systems, components and technical personnel interposed in between. These two modules at the extremes are very simple, auditable, open, and protected by physical and logical security. All the critical functions described below are realized in these two extremely simple modules.

The first module is the voting agent used by voters. It is a light-weight piece of software that can take the form of a digitally-signed applet of a couple hundred kilobytes, running in the voter's browser. The certification of such an applet avoids all of the complexity associated with the host operating system, the ballot presentation software, the network interface and so on. For improved security in remote electronic voting, the voting agent could run on a "clean" operating system version loaded from a bootable CD-ROM provided by the electoral authorities.

The second module is the electoral board agent. It consists of software, which is used to generate sensitive cryptographic keys and other critical data, and perform the critical process of opening digital ballot boxes, breaking the correlation between the voters and the contents of their ballots using cryptographic mixing processes [Cd81]. This software should be open, at least to the electoral authorities and political parties, which should extensively audit it. It runs on a very simple computer or specific-purpose hardware system, totally disconnected from any network and directly operated by election authorities and constantly monitored by several parties. Physical security is extremely important to protect this module.

A more detailed description of the security architecture introduced before, which was used in the Catalan pilot, can be found in [Ra03, SCT03]. Also, a summarized description of how the previously introduced security architecture addresses most of the security concerns raised in the SERVE security report [Jd04] can be found in [Ra04].

7 Concluding Remarks

Judging from the voter participation rates, survey results and the technical problems that were reported, we conclude that the 2003 Catalan electronic remote voting test pilot was a success. Given that this was a non-binding pilot where voters would have to vote twice to participate – once for real by mail, and a second time for the pilot by Internet – and where the promotion of the pilot was scarce, a 15.23% participation of postal voters can be considered as an excellent result. The participation rate demonstrated the interest among the voters in an alternative voting channel, as stated by many electors who indicated their predisposition to use this electronic system in binding elections in the future. The main objectives introduced at the beginning of this document, which reflect the main advantages of the remote electronic voting, were fully achieved, facilitating the participation of Spanish citizens living abroad with a secure and user-friendly e-voting system.

Another great success of the pilot was that it led to the identification of some areas of improvement, basically related to usability, and they have already been solved. The pilot also helped the Generalitat to detect some things not initially considered key in which remote electronic voting technologies can help: (1) to allow citizens who are not necessarily abroad to vote remotely, (2) to reduce the resources needed to manage the election, (3) to facilitate the management of the electoral rolls, and (4) to get voters' opinions on governmental actions between elections.

In the last few years, several governments around Spain and Europe have run different kinds of e-voting pilots, in order to test the technology and the social response to this technology. We believe that, after carefully considering the security and usability issues, the technology is mature and that the society demands it. Now it is time for legislators to step up and amend the, usually old, laws regarding electoral processes and citizen participation in order to cover the use of these new technologies

Bibliography

[GC03] Generalitat de Catalunya: Eleccions al Parlament de Catalunya 2003, http://www.gencat.net/governacio-ap/eleccions/e-votacio.htm. (In Catalan)

[Aa99] Ambrosio, A.: Electronic Voting Experiment, Generalitat de Catalunya, 1999.

[SCT03] SCYTL: Pnyx Electronic Voting System White Paper", http://www.scytl.com/voting.html

[Ra03] Riera, A. et al: Advanced Security to Enable Trustworthy Electronic Voting, Proc. 3rd European Conference on eGovernment (ECEG), Dublin, 2003.

[HD00] Hacker, L., J. Van Dijk: Digital Democracy. Issues of Theory and Practice, Sage Publications, London, 2000.

[Cd81] Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms, Communications of the ACM, vol. 24, issue 2, pp. 84-88.

[CM03] Canals, I., Martí, JL.: *L'Àgora Digital. Internet al Servei de la Participació Democràtica*, Fundació Catalunya Segle XXI, Barcelona 2003. (In Catalan)

[Ra02] Riera, A. et al: Electronic Government: Design, Application and Management (ed. Gröndlun A.), Idea Group Publishing, London 2002, pp 78-98.

[Jd04] Jefferson D. et al: Serve Security Report, http://www.servesecurityreport.org, 2004

[Ra04] Riera, A: Comments by Scytl on the SERVE security report, http://www.sctyl.com/docs/Scytl_comments_on_SERVE.pdf, 2004

[MN03] Mercuri, R., Neumann, P.G.: Verification for Electronic Balloting Systems, Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 31-42. Kluwer, Boston 2003.

[BM03] Burmester, M., Magkos E.: Towards Secure and Practical E-elections in the New Era, Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 63-76. Kluwer, Boston

Verifiability and Other Technical Requirements for Online Voting Systems

Niels Meißner, Volker Hartmann, Dieter Richter

Department of Metrological Information Technology
Physikalisch-Technische Bundesanstalt (PTB), Braunschweig and Berlin
Abbestraße 2 – 12
10587 Berlin, GERMANY
{Nils.Meissner | Volker.Hartmann | Dieter.Richter}@ptb.de

Abstract: When developing a catalogue of technical requirements for online voting systems to be used in legally ruled, non-parliamentary elections, major interdisciplinary problems arise which currently cannot be solved. Technical requirements are not yet definable due to lacking legal preconditions, and legal definitions are not yet definable due to lacking technical experience. Problems of this type are the role of a technically necessary intermediate storage of votes, the so-called last call problem and the general problem of ensuring verifiability. The problem of verifiability is discussed from the technical point of view to bring forward a possible solution[1].

1 Introduction

There are numerous application areas in which technical systems are subject to legal verification. The general aim is the protection of users, consumers or customers, respectively, who are usually not able to assess all possible risks. Electronic voting is one of those areas, and even a very sensitive one. Other areas are e.g. measuring systems used in commercial transactions and private households, and gaming systems.

Technical requirements play a key role in the management of regulated areas. Although in their shape of a technical nature, they are the most important interface between regulators and technicians, between developers and testers, between manufacturers and customers.

Looking at the situation in the area of electronic voting systems and, in particular, of online voting systems, it can be stated that there are several approaches to define requirements for online voting systems [JO00; UK02; NV02; CH03; US01; CE04]. In general, their state can be characterised as relatively general or not complete.

---

[1] The work is funded by the German Federal Ministry of Economics and Labour under the registration mark 01 MD 248.

This was the reason for taking the initiative to elaborate technical requirements for online voting systems. This initiative is embedded in a project of PTB funded by the German government, which aims at the development of concepts for testing and certifying online voting systems to be used in legally regulated, but non-parliamentary elections (e.g. elections of shop committees, staff councils, shareholder elections).

This paper aims in its main part, section 4, at the problem of verifiability as one of the major problems of online voting systems. Before, in section 2, the catalogue of requirements is briefly explained. The catalogue has been developed at PTB and discussed in two national working groups. One of these groups is dealing with technical aspects of testing and certification, the other one with legal aspects. In section 3, major interdisciplinary problems are described which were fixed in discussions in the two working groups.

2 The catalogue of requirements

The catalogue of requirements [HM04] gives criteria which are to be met by online voting systems. Its purpose is to set a technical standard which can serve as an orientation for both, developers and examiners of online voting systems. Well-defined requirements are, in particular, a precondition for the examination and certification of systems, which have to be performed carefully in order to build confidence in the systems.

Even though the state of the art is progressing both from the technical point of view and as regards the acceptance of online voting systems by society, the catalogue is intended to provide some guidance on the requirements presently acceptable.

The second reason for developing the catalogue is to contribute to the ongoing discussions on online voting systems. The document represents expertise and opinions from different backgrounds in Germany. It may be considered as a reference for further activities.

The scope of application is given by legally ruled non-parliamentary elections. The requirements are also applicable to any other non-parliamentary type of election not regulated by law, whereas one or another requirement might be weakened. As to the application in parliamentary elections, the authors are convinced that most of the requirements are also valid. Particular analysis, however, is necessary to decide on potential extensions of the requirements.

For the definition of the requirements, it has been assumed that elections take place exclusively at supervised and networked polling stations. Applications allowing voting from at home or any other private place are explicitly not included in the definition.

3 Selected Legal Questions

Basically, any set of technical requirements represents a certain interpretation of the general legal requirements given. An interpretation shall follow as close as possible the initial legal intention. However, if the general legal requirements are not yet defined or only very roughly defined – as it is the case with some aspects of online voting systems – then problems arise with the definition and harmonisation of technical requirements. Three major problems of this type are described in the following subsections.

3.1 The role of an intermediate storage

Online voting systems have a feature that is unknown in conventional voting systems: It is the physical state of an (encrypted) vote after having finally completed its electronic casting at the voting terminal and before putting it into the electronic ballot box. This state may last only a fraction of a second but can also, in case of a communication interruption, last for several minutes or even hours. In the latter case, the vote must be stored and held ready for communication in an intermediate storage. An intermediate storage could also be regarded as a conceptual element of the voting system used, for instance for the management of a certain vote transfer protocol.

The main question that arises concerns the legal definition of an intermediate storage. One may ask what the intermediate storage is from the legal point of view? Is it an episode of the vote transfer process, is it already part of an extended ballot box or is it still part of the vote casting? The answer to these questions has an impact not only on the technical requirements for an intermediate storage but also on the answers to related questions as e.g. with respect to the registration of vote casting in the list of voters, feedback from a successful input into a ballot box to the voter.

3.2 The last call problem

A special problem of voting systems with distributed components is the harmonisation of the beginning and the end of the vote casting. Aside from the clear definition of deadlines to be given for the vote casting, the closing procedure must be defined. In particular, it must be ensured that no vote that has been cast regularly within the defined deadlines will be excluded from vote counting. This means that the ballot box must not be closed for the reception of further votes until it has been ensured that no further regular vote is “in the air.”

The technical solution relates to the solution of an intermediate storage described in the previous subsection. The legal problem is to what extent the solution of the last call problem must be prescribed. This question is very sensitive because complaints directed against the incompleteness of votes considered due to a technical failure of the system are very likely. The general aim from the legal point of view is to ensure and prove the completeness and correctness of an election result. The proof shall pass a verification. In so far, the last call problem is a special aspect of a more general problem of verifiability described in the next subsection.

3.3 Verifiability

Verifiability is an essential feature of an election demanded by electoral jurists. It is linked with such aspects as confidence in the election, transparency and preparation for a possible contestation of the election. There are different types of verification. The difference may be characterised by the groups of persons who are authorised to access the information gathered for verification (audit information). The variation reaches from everybody interested (public verifiability) to voters, election officials only and independent auditors to court only. A verification by court is usually caused by complaints that the results of an election were not correct or that the election has not been executed according to the rules.

In general, the technical problem can be described as the definition of the necessary technical measures that are required to pass a verification. So far, however, there is neither a definition nor any practical experience as to what kind of technical proof and evidence is sufficient for a verification. This explains the difficulty technicians and legal experts are currently facing.

4 Selected problem: Ensuring verifiability

4.1 Basic considerations

Basically, the verifiability is, on the one hand, a matter of designing a technical audit and, on the other hand, a question of correctness proofs. An audit needs to be specified with respect to, e.g., the information content to be observed and logged, data structures, security measures, etc. Correctness proofs are closely related to the anonymisation methods used. A basic principle that must be regarded and must never be violated is the sanctity of the anonymity.

As regards the audit, approaches are known from auditing sensitive systems. In particular, the security of audit logs is well treated in literature [BE97; CP03; GA87]. However, so far no specific approach for electronic voting systems is known. It seems to be clear that an auditing must address two aspects: the path that a vote takes through the network-based online voting system and the technical states of the components of the electronic system during the whole voting process. In particular, all abnormal technical states must be logged in order to be able later to judge whether the conformity of rules was kept.

An approach currently discussed in the USA is the so-called paper audit trail. The content of the vote is printed before the vote casting is finally completed. Then the correctness can be verified by the voter. If everything is correct, the print-out is put into an additional ballot box and the electronic vote is stored. In case of a contestation of the election, the paper ballots can be counted separately and used for the verification. This principle results in an additional complexity and source of errors such as, for example, jamming of printer paper, empty printer cartridge, etc. In addition, in case of a contestation, the lengthy, fault-prone hand counting remains.

This approach will not be further discussed here. Rather, initial ideas are outlined how the audit can be organised with the blind signature type encryption and with the homomorphic encryption type.

4.2 Principle applicable for systems using blind signature encryption type

Some systems [IV02; KK02] use blinded signatures [CH83] to secure the anonymity of the votes (Figure 1). [IV02] works as follows: After having identified and authenticated the voter, he/she gets signed electoral documents from the election server. The signature is necessary to ensure the protection of data integrity. After having filled in the ballot, the voter blinds the vote, i.e. he/she multiplies the data by a random number and sends the thus blinded vote back to the election server. The server signs the blind vote without being able to see the voting decision and sends it back to the voter. The voter removes the blinding, i.e. he/she divides the blind signature by the blinding factor to get a signature of his vote. He/she then encrypts the vote and the signature with the public key of the tallier and sends the data to the ballot box. Either the transmission takes place anonymously or the vote is made anonymous by the ballot box server stripping away voter ID information. After having closed the vote casting, the anonymous votes and signatures are sent to the tallier which decrypts them separately. Only votes with a valid signature of the election server are counted.

In the algorithm in [KK02], two tokens and not the vote are blindly signed in the registration phase. These signed anonymous tokens allow the voter to receive the ballot and vote anonymously later in the voting phase.

Unlike the systems that use homomorphic encryption (see 4.3), these systems have no inherent verification mechanism. Therefore an additional mechanism has to be embedded to ensure verifiability.

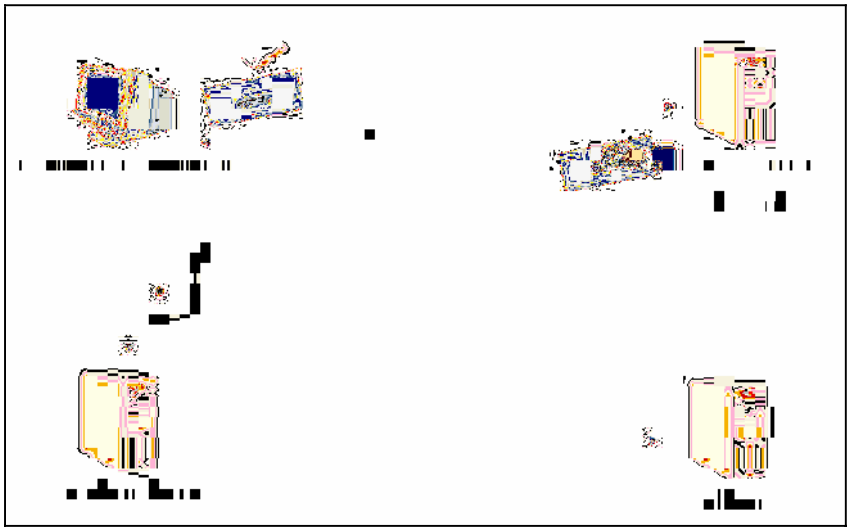


Figure 1: Schematic view of an Online Voting System using blind signatures

For the support of the verification, additional information and effort are necessary. A possible approach is illustrated in Figure 2. This figure shows how the proper execution of the election can be documented. The basic idea is to design an audit data set, which is logged with all single steps during the "lifetime" of a vote. A part of this audit data set is a token, which serves for the identification of the individual vote cast.

This token is generated at the time when the voter has been accepted as eligible for voting. Simultaneously, it is encrypted with the public key of the auditor and inserted into the audit data set. This structure is signed and sent to the voter together with the electoral documents (ballot, etc.). From this moment, the audit data set accompanies the encrypted vote. At each relevant point passed by the vote data, the audit data set is enriched with the necessary audit information and signed again by the appropriate entity. When reaching the ballot box, the audit data set is separated from the vote data and stored separately. To guarantee verifiability, the audit data sets are sent to the audit box during or after the election and the tokens are decrypted. With this information, each individual vote casting can be reconstructed by using the token and the signed audit information.

The anonymity of the vote is not endangered because of the strict separation of the audit data from the content of the vote through encryption. The information content of the audit data to be gathered depends on the subject of possible verifications and may be adapted to the particular needs. The correct counting of the votes, however, cannot be verified by the approach developed here.

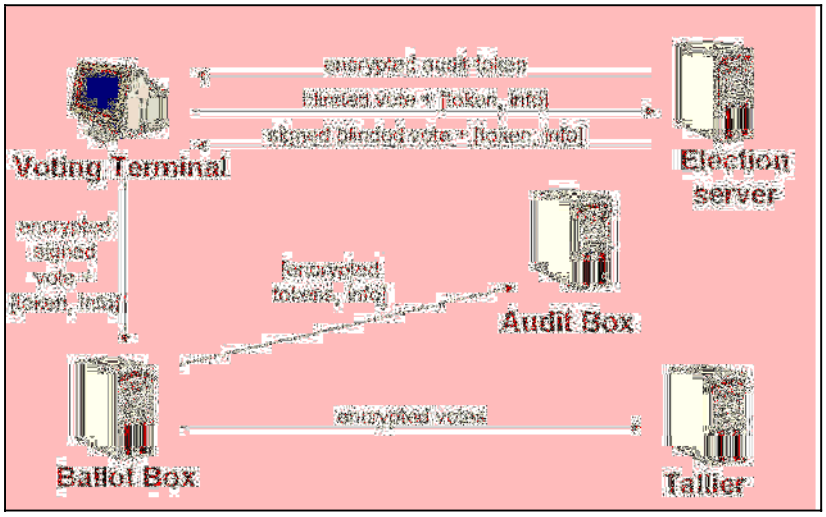


Figure 2: Schematic view of the audit data set approach

4.3 Principle applicable for systems using a homomorphic encryption type

Voting systems using homomorphic encryption [CY99; VH02; CG97], Figure 3), work with a communication model called bulletin board. It is a public broadcast channel with memory. All information sent to the bulletin board is readable by everyone. Every authorised user can add messages to his own area, but no one can delete any data from the board.

The central element of the homomorphic encryption is the feasibility to sum up data without encrypting them, i.e. without knowing the exact content of the data. This is a feature that is typical of the principle of homomorphism. More precisely speaking, the homomorphic encryption ensures the mathematical law that the product of encrypted data is the encryption of the sum of the data:

$$Enc(v_1) *...* Enc(v_n) = Enc(v_1 +...+ v_n).$$

The method works as follows: Before the election, the talliers generate distributed asymmetric keys (e.g., [PE91; GJ99], threshold cryptography). These keys are a single public encryption key and for each tallier a secret decryption key. To decrypt a message encrypted with the public key, more than at least half of the secret keys have to be used. Therefore more than half of the talliers would have to be corrupted in order to break the anonymity or manipulate the election result.

Only authenticated voters are allowed to write on the bulletin board. The voters send their votes encrypted with the public part of the distributed key to the bulletin board, together with a zero knowledge proof of correctness. After the voting phase, the talliers take all the encrypted votes from the bulletin board and form their homomorphic sum. Afterwards this sum is decrypted using the distributed parts of the key and sent to the bulletin board with proofs of correctness of the summation and the decryption. By skilful

application of zero knowledge proofs, and because everybody (even external observers) can read the information on the bulletin board, everyone can verify the correctness of the results. This includes the correct summation and the completeness of votes included.

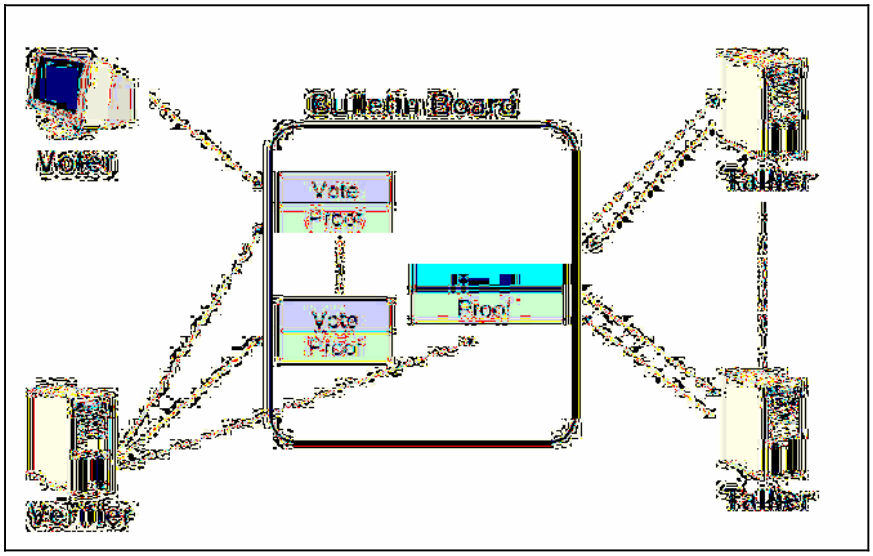


Figure 3: Schematic view of an online voting system using homomorphic encryption

Online voting systems with homomorphic encryption secure, in particular, the casting of correctly formed votes as well as a correct counting. This is verifiable during the election, and, in addition, remains verifiable after the election. However, this encryption type cannot monitor the proper execution of the election. In order to trace the execution, an additional audit logging is necessary. Since the information on the bulletin board can be used for verification, less information is probably needed for the audit logging compared with systems that use blind signatures.

5 Conclusions

Technical requirements of online voting systems have been developed and discussed in a community with different expertise and experience. There are still several unsolved interdisciplinary legal and technical problems left. Sufficient technical experience does not yet exist to decide profoundly on the respective legal aspects. Vice versa, there is no clear legally defined background as an initial point to solve the technical problems. This looks like a deadlock situation. From the technical point of view, this situation can be overcome step by step by assuming certain legal conditions required, then specifying the technical issue to be dealt with and implementing corresponding components or methods. From the experience gathered, feedback can be given to evaluate and adapt the initial legal assumptions. This is the way that has been chosen with the discussion of verifiability in section 4. A new technical approach to ensure the verifiability of voting systems that use blind signatures was presented.

References

[BE97] M. Bellare, B. S. Yee: Forward Integrity For Secure Audit Logs, 1997, http://www.loganalysis.org/sections/research/fi.pdf

[CE04] Council of Europe: Draft - Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, http://www.coe.int/t/e/integrated_projects/ democracy/02_Activities/02_e-voting/

[CG97] R. Cramer, R. Gennaro, B. Schoenmakers: A secure and Optimally Efficient Multi-Authority Election Scheme, Advances in Cryptology – EUROCRYPT'97, Vol. 1233 Lecture Notes in Computer Science, Springer Verlag, 1997, pp. 103-118

[CH83] D. Chaum: Blind signatures for untraceable payments., Advances in Cryptology – Crypto'82, Plenum Press, 1983, pp. 199-203

[CH03] Verordnung über die politischen Rechte vom 24. Mai 1978 (as of 28 January 2003), 161.11, http://www.admin.ch/ch/d/sr/161_11/

[CP03] C. N. Chong, Z. Peng, P. H. Hartel: Secure Audit Logging with Tamper-resistant Hardware, SEC 2003, 73-84, http://www.ub.utwente.nl/webdocs/ctit/1/00000099.pdf

[CY99] CyberVote, an innovative cyber voting system for Internet terminals and mobile phones, IST-1999-20338, www.eucybervote.org/reports.html

[GA87] P. R. Gallagher: A Guide to Understanding Audit in Trusted Systems, NATIONAL COMPUTER SECURITY CENTER, NCSC-TG-001, VERSION-2, Library No. S-228,470, 1987, www.radium.ncsc.mil/tpep/library/ rainbow/NCSC-TG-001-2.pdf

[GJ99] Gennaro, Jarecki, Krawczyk, Rabin: Secure Distributed Key Generation for Discrete-Log Based Cryptosystems, Advances in Cryptology – EUROCRYPT'99, Vol. 1592 Lecture Notes in Computer Science, Springer Verlag, 1999, pp. 295-310

[HM04] V. Hartmann, N. Meißner, D. Richter: Online Voting Systems for Non-parliamentary Elections - Catalogue of Requirements, PTB, 2004, work in progress

[IV02] Erste verbindliche Online-Wahl im LDS – Abschlussbericht über Online-Personalratswahl im Landesbetrieb für Datenverarbeitung und Statistik (LDS) Brandenburg im Mai 2002, www.i-vote.de

[JO00] B. Jones: California Internet Voting Task Force, A Report on the Feasibility of Internet Voting, January, 2000, www.ss.ca.gov/executive/ivote/

[KK02] R. Kofler, R. Krimmer, A: Prosser: Electronic Voting: Algorithmic and Implementation Issues, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), 2002

[NV02] Network Voting System Standards (Public draft 2 – 12.04.2002), VoteHere, Inc. www.fec.gov/pages/vss/comments/NetworkVotingSystemStandards.pdf

[PE91] T. Pedersen: A threshold cryptosystem without a trusted party., Advances in Cryptology – EUROCRYPT'91, Vol. 547 Lecture Notes in Computer Science, Springer Verlag, 1991, pp. 522-526

[UK02] e-Voting Technical Security Requirements, Issue 1.0, 08 November 2002, X/10049/4600/6/21, Crown Copyright, http://www.odpm.gov.uk/stellent/groups/ odpm_localgov/documents/page/odpm_locgov_605209.pdf

[US01] Voting System Standards, 2001, www.fec.gov/pages/vss/vss.html

[VH02] www.votehere.net (Demo, www.votehere.net/products_rv.htm#demo)

From Legal Principles to an Internet Voting System

Melanie Volkamer, Dieter Hutter

German Research Center for Artificial Intelligence GmbH
DFKI Saarbrücken
66123 Saarbrücken, GERMANY
volkamer@dfki.de, hutter@dfki.de

Abstract: Past research on Internet voting has been concentrated on two aspects. First, there are investigations to find the appropriate balance between anonymity and authentication. Second, the impact of the use of Internet voting to legislation has been studied. In this paper we analyze the impact of legislation to the design of a real Internet voting system. We discuss how legal aspects constitute security requirements on a technical level and refine the security requirements on the design level to corresponding security requirements of the resulting system.

1 Introduction

Reforms of the execution of democratic elections have taken place several times in the past. In the advent of e-democracy and e-government initiatives, the question arose whether and how citizens can be entitled to use the Internet in order to participate in elections. In the last years various voting systems, like for instance the i-vote system [FGr] in Germany, have been developed and tested in various countries. The popularity of Internet voting reached its peak in 2001. However, at the same time the difficulties in developing a legal voting system satisfying the required security properties have become obvious.

There are various proposed approaches for Internet voting (see [Sch96] for an introduction). We distinguish between Internet voting systems using polling stations and those allowing the voters to use their own personal equipment. With respect to the authentication to the system, a voter can legitimate herself either by presenting her PIN (or TAN) codes or by using an existing digital signature infrastructure. Systems also differ in the characteristics of the components an user has to trust in when using the system or they differ in the used cryptographic algorithm.

Since voting systems are complex distributed systems, it is rather difficult to understand up to what degree the system will guarantee the required security properties. Furthermore, up to now there are no standard criteria available, like for instance a Common Criteria Protection Profile [ISO00], to evaluate and certify Internet voting systems.

That is why developing an Internet voting system that is accepted by the voters and that also satisfies all requirements in a traceable way is still an unsolved task.

In this paper we use the basic methodology of the Common Criteria to develop technical requirements for a suitable voting system from the given legal preconditions that are formulated in electoral laws and constitutions. We start with the discussion of the legal principles in chapter 2 and develop a trust model based on these legal principles in chapter 3. Using this model we deduce compulsory requirements for the system design in chapter 4. In chapter 5, we present our Internet voting system *SecVote* and investigate in the next step the mechanisms to meet all requirements set up by the trust model. Finally, chapter 6 gives some details about the implementation of this system.

2 Legal Principles

The touchstone in developing an Internet voting system is represented by the necessity to meet the requirements of legal principles ([Wil02] for an introduction). In Germany, like in many other democracies, all elections have to satisfy basic voting principles which are formulated in constitutions and electoral laws. Elections have to be **universal, equal, free, secret** and **direct**.

The principle of **universal** elections guarantees equal suffrage for everybody which also means equal access to voting. For instance, it is not allowed to exclude any persons subgroups from an election. **Equal** elections guarantee that all ballots have the same influence on the result. Furthermore, voters are able to vote in the same formal way. The principle of **free** elections requires the facility for every voter to cast her ballot free of duress and without unlawful and undue influence. In particular this implies that a voting system must anticipate that a voter can be influenced by leaking intermediate results of an ongoing election. **Secrecy** of elections demands that only the voter is aware of her voting decision, which may never revealed to anybody else without her permission. To prevent disposal of votes the voter must not be able to prove anybody the result of her voting. The principle of **direct** elections prevents someone from voting on behalf of other eligible voters or the use of an electoral college.

3 Trust Model

In this chapter we derive the trust model from the legal principles presented above. We assume two groups of persons interacting with the voting system. First there are people who are interested in the correctness and security of the system: “honest” voters using the system and the organizers of the election maintaining the system. Second there is a malicious attacker who might be also camouflaged as a voter or an organizer.

We assume that this attacker is very powerful: He is able to read, save and delete all protocol messages - especially all transmitted ballots. The attacker can generate new messages or modify intercepted messages and send them to arbitrary system components. He is computationally restricted with respect to his computing resources during the election but we act on the assumption that an attacker might be able to overcome this restriction in the future. The attacker can also observe who actually is in the polling station at a given point of time. Equipped with these abilities, he tries to corrupt the secrecy of the votes of specific individuals, to manipulate the result of the election or simply to obstruct the election in general.

Honest groups act in compliance with the rules of the voting system and assist in detecting any kind of election fraud. These participants have two kinds of requirements: system requirements and those to the environment. So we developed an Internet voting system satisfying the legal principles if environmental requirements are guaranteed.

3.1 Requirements to the system

In the following we derive the **system requirements** of a voting system by analyzing the legal principles more closely:

The principle of **universal** election requires that the voting system is available for all voters independent of their personal holdings, can be used by all voters without requiring special knowledge, for instance in computer science, does not lose any data (e.g. during ballot transmission), and counts all ballots correctly.

Availability of the voting system implies that it must never enter an undefined state and that there is a trustworthy backup mechanism to recover the system in case of an emergency, e.g. a hardware failure.

The principle of **equal** election results in the need to prevent unauthorized access to the system. Voters have to authenticate themselves, each person can only vote at most once, and each ballot is counted exactly once within the result. As a consequence attackers must not be able to modify, copy or generate ballots without being detected by the organizers.

The principle of **free** voting means that attackers must not be able to influence a voter's decision which implies that it must be impossible to observe the voter in her decision. Also voters must not be able to prove their own decision to someone else because otherwise they might sell their votes. Until the election deadline is reached, the ballots must be transmitted and saved confidentially to prevent the calculation and publication of intermediate results.

The principle of **secret** election requires that any mapping of a voter to her ballot must be impossible during the election but also for the future. We have to take into account that both, the computational resources as well as the knowledge on cryptography will steadily increase in the future.

This requirement will essentially influence the design of ballot transmission and storage. The principle of secret election is an essential precondition for free voting.

There is no technical proviso for Internet voting with respect to the principle of **direct** elections.

Summing up, there are far more requirements arising from legal principles than ensuring secrecy and integrity of individual votes as it is often mentioned. Furthermore it is important to notice that the secrecy of election must be unconditionally ensured forever regardless of ongoing technological improvements.

3.2 Preconditions to the environment

Internet voting systems are technical systems which will only operate correctly if the environment is able to guarantee certain preconditions. For example, software systems requires dependable hardware which itself depends on a reliable power supply. Analogously, we have to assume certain preconditions on the environment in which the voting system will run to ensure the security of the overall system.

We assume that an attacker will only be able to manipulate a single component of the voting system. Our approach has to guarantee that the malicious corruption of a single component will be either detected during the election or else will not inflict the security of the system. The rationality behind this assumption is that the different components will be distributed on different locations and different persons will be in charge to maintain and supervise them. So we assume that organizational means will make sure that persons in different positions and locations will not collaborate in corrupting the system. Additionally we also suppose that people from different lobbies, who share a secret, do not work together to manipulate the election (principle of separation of functions and dual control). Furthermore, we assume that more than one voter casts her vote and not all votes are identical. Moreover we suppose that not all voters apart from one will conspire against the remaining voter to find out her decision.

Additional requirements are that the components are secure platforms (e.g. using a secure Linux version only equipped with the voting software) because otherwise we would have to trust in all other installed software and there might be a lot of possible attacks caused by Trojan horses. Such a program could cast the vote without voter's knowledge or it could even change the voter's decision before sending the ballot. Another possibility would be that the Trojan horse would send the voter decision directly to the attacker. Consequently the attacker reaches his goals independent from the system architecture and the used protocols.

Having these requirements to the system and the preconditions of the environment in mind, we will illustrate the necessary design decisions of our Internet voting system in the next chapter.

4 Design

As illustrated in the introduction there is a variety of alternative solutions to design an Internet voting system. However, not all of them will meet the requirements given in chapter 3. Some of the design decisions are indispensable:

Polling Station vs. Individual Computer Internet voting must take place at the polling station at present because the use of individual computers is not conformable with the requirement that everybody can vote regardless of her personal havings and it also violates the assumption that only trusted secure platforms must be used. We cannot guarantee the absence of Trojan horses on personal computers which might corrupt the secrecy and integrity of the overall system.

Authentication A next design decision concerns the issue of authentication. The use of digital signature cards combined with personal identification numbers (PIN) currently is the best compromise between security and minimizing the resulting costs of implementing the technology (compared for instance with using personal fingerprints). Using qualified signatures, as described for instance by the German Digital Signature Act, the requirements for authentication can be satisfied. This aspect implies another design decision: it is essential to establish a certificate authority that creates the certificates to check the validity of the voters signatures.

Divison of Power Each voting system must respect the principle of the division of power because otherwise (as we assumed in the definition of our trust model) an attacker would be able to corrupt the system by manipulating the single component. It is important to notice that the division of power enforces the separation of computations in the following three situations: Two components are needed for authorization check. A single component would permit unauthorized people to vote or to exclude authorized voters from voting, for instance, by changing the electoral register. This would contradict the requirement that an attacker is not successful if he manipulates only a single component.

The second situation occurs within the polling booth. Because we require that votings are kept secret and assume that an attacker can manipulate a single component, we also need two components in the polling booth. One component is concerned with the registration and the processing of voter's information and the other component is casting the votes without knowing anything about the actual voter. Even if one of these components is attacked, there is no allocation from the voter to her decision possible. Finally, it is essential to separate ballot collection from result calculation to prevent the calculation of intermediate results. This means that there is a component which simply collect all ballots but which is not able to calculate intermediate result. After reaching the election deadline all ballots are transferred from this component to a second one which will calculate the result of the election.

Beyond Cryptographical Secrecy There are two additional design aspects from the given legal requirements: The first aspect is concerned with the electoral secrecy which must be guaranteed also in the future. It is hard to predict how progress in computer hardware and cryptography will damage probabilistic properties of existing cryptographic approaches. Additionally, we assume that the attacker is able to read all transmitted ballots and he can observe who actually is in the polling booth at a given point in time. Therefore it is not sufficient to use encryption - neither asymmetric nor symmetric - if the component transmits the ballot immediately. An attacker will know the allocation between voter and her decision as soon as the underlying cryptographic approach is broken. A new mechanism similar to MIXEs [Cha81] is needed to conceal the relation between a voter standing in the booth and the votes being sent from one component to another. We will discuss the details of our mechanism in the following section. However, even if we use such a mechanism, the encryption of ballots is still essential for another reason: to prevent intermediate results, which must be confidential until the end of the election (This encryption is the second design aspect).

Summing up, the architecture of the proposed Internet voting system consists of two components which check the authorization, one component to collect the votes and another one to compute the result. Furthermore, there are two components in each polling booth. One component is concerned with the authorization of the voter while the other component is used for the actual voting.

5 Realization

Based on the analysis presented above, we developed an Internet voting system called *SecVote*. In this section we will describe the architecture of the system (cf. Figure 1) which consists of the following six components:

The **Registration Server** (RegServer) and the **Certificate Authority**[1] (CA) that are responsible for authorization check, the **Voting Box Server** (BoxServer) that collects the votes and stores the content of all ballots, and the **Control Server** (Controller) that computes the final result. The **Registration PC** (RegPC) that deals with the authentication for access and the **Voting PC** (VotePC) to cast the voter's ballot (both in the polling booth).

Protocol The protocol (cf. Figure 1) of the voting process works as follows: The voter enters the polling booth and is informed by the RegPC to activate her signature card using her individual PIN code.

[1] The Certificate Authority is used for two tasks: first to check the cert validity and second for the authorization of voters.

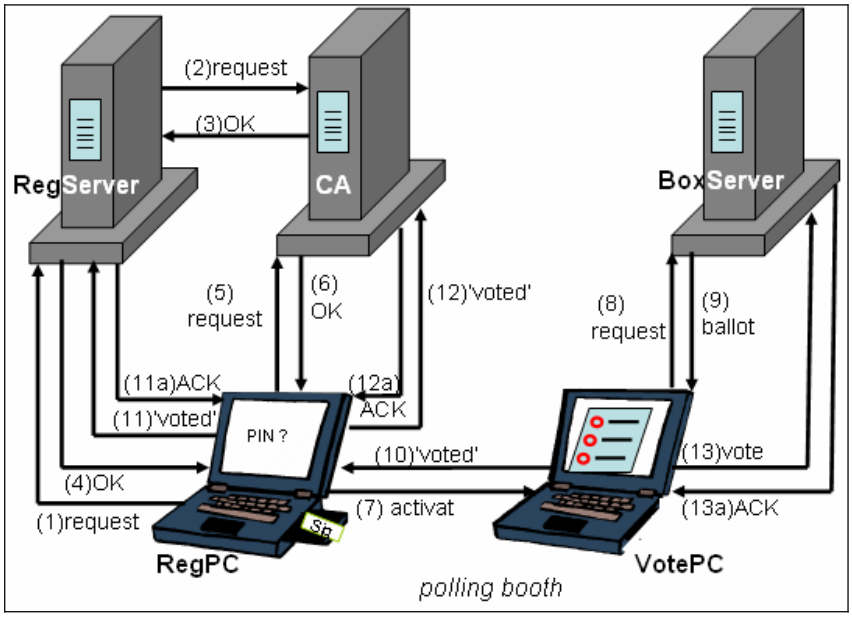


Figure 1: Architecture and Communication

The RegPC sends a request both, to the RegServer (1) and to the CA (5). Receiving the query, the RegServer checks the voting authorization and sends a validity request to the CA (2). The CA, getting the message, checks it against its revocation list to see whether the cert is still valid, and sends the answer back to the RegServer (3). The RegServer forwards this answer to the RegPC (4). In addition the CA receives a request directly from the RegPC (5). Before sending the answer to the RegPC (6) it checks the voting authorization and the cert validity. If the RegPC receives the acknowledge from both components, RegServer and CA, it sends a message to the VotePC (7) to activate the voting process and informs the voter that she should proceed to the second PC. This PC first asks the BoxServer for the content of the ballot (8) and displays it to the voter after receiving this information (9). Next the voter has to make her decision and to acknowledge it. Then, the VotePC informs the RegPC (10) to change the status of the actual voter in the election register and sends the ballot to the BoxServer (13). The RegPC forwards the information about the end of the actual voting to the RegServer (11) and the CA (12). Both components adjust their internal database and send acknowledgments to the RegPC (11a, 12a). The BoxServer stores the ballot and acknowledges it (13a). Both, VotePC and RegPC display a message that the ballot was casted successfully and that the voter can remove her signature card. The system is now ready to welcome the next voter in the polling booth.

The sketched design of the system (architecture and protocol) is not sufficient to ensure the given overall requirements. Additional mechanisms are needed to meet these requirements. Some of them are obvious: e.g. all messages have to be digitally signed to

obtain integrity and authenticity. A back-up-system is required to safeguard the availability of the system, access control mechanisms are necessary to gurantee the privacy and integrity of data on individual hosts, and mechanisms are needed to ensure secure data transfer.

Secrecy of election and uniqueness of ballots This section will illustrate the mechanisms used in *SecVote* to keep the **election secret** and to prevent that ballots are deleted, changed or added. The main problem with the secrecy of elections is the assumption that eventually in the future an attacker will be able to decode the recorded encrypted votes sent from the VotePC to the BoxServer. Although the votes do not contain any information about the voter, the attacker might still be able to monitor the polling station and relate the physical presence of a voter in the polling station with the shortly following message of the VotePC to the BoxServer.

Therefore, we use a similar approach to MIXEs [Cha81]. The VotePC does not immediately transmit the voter's ballot but the first casted ballot is only stored within the VotePC. Two ballots always remain in the memory until the next person casts her vote. The VotePC transmits now one of these two to the BoxServer. The choice is absolutely random. Thus an attacker does not know whether the transmitted ballot correspond to the first or to the second voter. He can only make a guess with a probability of 0.5. The same procedure takes place for the following voter and all others. After finishing the election the VotePC sends the last stored ballot to the BoxServer. This ballot can be either from the first, the last or any other voter. Hence the attacker, once able to crack the cryptography, only knows that either the last or the last but one transmitted vote belongs to the last voter in the polling station.

There is one case in which the attacker will know the decision of the last voter in the election once he is able to decode the encrypted messages: If the last and the last but one transmitted ballot are equal then the attacker is able to allocate this decision to the last voter of the election. However, on the one hand the probability of this event is very small[2] and the attacker cannot precipitate such a situation. On the other hand the attacker only knows about the decision of a randomly affected voter but cannot use this weakness to get hold of the decision of a previously selected person. So this fact does not affect the trust model and the proposed procedure can be used to safeguard the secrecy of the election.

Within *SecVote* we have incorporated three mechanisms to **ensure the correctness of the voting result**: To prevent that ballots are copied or modified, all messages are signed together with a unique random number. The Controller verifies all signatures and checks that all numbers are unique. Apart from that, the Controller compares also the number of received ballots with the number of voters in the election register from the CA and the RegServer. Thus, any deletion of votes will be revealed. To ensure that the VotePC transmits or stores the correct ballot, the signature is generated on an external secure signing component (Signierkomponente) equipped with a separate screen.

---

[2] The probability depends on the number of possible votes and becomes exponential smaller if you collect more than two votes before sending once.

6 Implementation

SecVote was implemented as a proof of concept of the presented design of an Internet voting system. It includes most of the functionality outlined in this paper and was implemented in a collaboration between the Federal Office for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik) and the German Research Center for Artificial Intelligence (Deutsches Forschungszentrum für Künstliche Intelligenz).

Its main parts are implemented in Java. The used cryptographic algorithms are RSA [RSA78] with SHA-1 [NIS92] for digital signatures, IDEA [Lay92] for symmetric encryption and a pseudo random number generator from Sun - however for a legal election it must be replaced with a perfect random number generator.

7 Related Works

There is a vast number of literature concerning Internet voting, the development of systems and the test of resulting systems. The published work can be divided into work on Internet voting (including suitable protocols for communication) allowing voters to use their individual personal computers and work on voting based on polling stations.

Examples for individual Internet voting are described in [Sch00] and [Cha81]. However, this class of voting systems, which will run on non-trusted hardware, does not conform with the legal standards presented before. The emphasis of most of these papers was put on two requirements: to ensure the secrecy and the integrity of the election. They abstract from the unsolved problem of voting using untrusted hardware and operating systems and the problem of ensuring that all voters are equipped with the necessary systems. However, without solving these problems the use of these proposed systems would lead to a violation of the principle of universal suffrage.

The other group of papers is addressing the problems of individual platforms and propose the use of polling stations for voting systems. Most of these voting systems, like for instance [FOO93], [PKKU02] and [BY86], adopt the principle of the division of power. These voting systems fulfill at least some of the mentioned design decisions. But they do not unconditionally ensure the election secrecy. They use, for instance, only encryption to ensure the secrecy of ballot transmission (e.g. i-vote [IVO02] uses RSA) but neglect the fact that any used encryption mechanism based on probabilistic results might be cracked in the future. It is insufficient only to separate votes from information about the voters. This could result in a violation of the legal principles in the future.

Besides the design of these systems there are additional problems arising with the implementation of such existing Internet voting systems. To ensure economical success, developers of these systems do not publish detailed information about the system and do not speak about the source code. Since these systems are also not certified by a trusted third party, voters will have to trust in the developers that everything works correctly. But this lack of control results that most voters will not accept such systems.

8 Conclusion

In this paper we illustrated how to develop an Internet voting system for legal and binding elections. This proposed system is in accordance with German laws, which are very close to those in other European countries. The described design, following the principle of division of power for the design of the architecture and inventing a random-mechanism for transmitting ballots, ensures legal standards and especially the unconditional secrecy of the election regardless of future developments in cryptography. Furthermore our system is robust in a sense that it will notice forgeries even if the attacker is able to manipulate a single component.

Literaturverzeichnis

[BY86] Benaloh, J. C.; Yung, M.: Distributing the Power of a Government to Enhance the Privacy of Voters; In: Proc. 5th Symposium on Principles of Distributed Computing (New York, USA: ACM 1986), pages 52-62,1986.

[Cha81] Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, University of California, Berkeley -Communications of the ACM, 24: 84-88, 1981.

[FGr] Internetseiten der Forschungsgruppe Internetwahlen mit Informationen zur Software und zu den durchgeführten Projekten; www.internetwahlen.de.

[FOO93] Fujioka, A.; Okamoto, T.; Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections; In Advances in Cryptology - AUSCRYPT 93; Springer-Verlag; pages 244-251; 1993.

[ISO00] ISO/IEC International Standard; Common Criteria for Information Technology Security; Evaluation (CC); Version 2.1; ISO IS 15408; csrc.ncsl.nist.gov/nistpubs/cc/; 2000.

[IVO02] Abschlussbericht zur Online-Wahl im Landesbetrieb für Datenverarbeitung und Statistik im Land Brandenburg; www.forschungsprojekt-wien.de/pdf/lds.pdf; page 23; 2002.

[Lay92] Lay, X.: On the design and security of block cipher; In ETH Series in Information Processing; 1992.

[NIS92] NIST: Proposed Federal Information Processing Standard for Secure Hash Standard – FIPS; National Institute of Standards and Technology (NIST); 1992.

[PKKU02] Prosser, A.; Kofler, R.; Krimmer, R.; Unger, M. K.: e-Voting.at: Entwicklung eines Internetbasierten Wahlsystems für öffenliche Wahlen; Arbeitspapiere zum Tätigkeitsfeld Informationsverarbeitung und Informationswirtschaft; 2002.

[RSA78] Rivest, R.;Schamir, A.;Adleman,L. M.: A Method for Obtaining Digital Signature and Public-Key Cryptostreams; In Communications of the ACM; 1978.

[Sch96] Schneier, B.; Applied Cryptography; John Wiley & Sons; 1996;

[Sch00] Schoenmakers, B.: Fully Auditable Electronic Secret-Ballot Elections; 2000.

[Wil02] Will, M.: Internetwahlen - Verfassungsrechtliche Möglichkeiten und Grenzen; LL.M. (Cambr.), Institut für Öffentliches Recht Philipps- Universität Marburg; Richard Boorberger Verlag GmbH & Co; Recht und neue Medien Band 2; 2002.

How Security Problems Can Compromise Remote Internet Voting Systems

Guido Schryen

Institute of Business Information Systems
RWTH Aachen University
Templergraben 64
52062, Aachen, GERMANY
schryen@winfor.rwth-aachen.de

Abstract: Remote Internet voting systems still suffer from many security problems which rely on the clients, the servers, and the network connections. Denial-of-service attacks and viruses still belong to the most challenging security issues. Projects and studies like the "Voting Technology Project" of CALTECH and MIT or SERVE of the US Department of Defense set up to gain experience evidence many of the notional weaknesses of current Internet voting systems.

1 Introduction

Theoretical research about the security of electronic voting systems started many years ago and countless approaches have been proposed since then. Not only motivated by academical research, but also quickened up by the US-presidential election's dilemma in 2000 several practical projects were conducted to assess the feasibility of electronic voting systems over the Internet. But reducing election problems to the counting process itself – as it might happen due to the big election in 2000 – clouds some more issues to be faced. How many votes have been destroyed, how many eligible voters have been disenfranchised from voting, how many votes have been altered in the context of absentee voting? Most people trust in the established offline voting procedures and show little interest in security issues as long as computers and networks are not involved. Actually, the real extent of election fraud is undetected, only some are known and published. The report of CALTECH and MIT [CM01, p.3] mentions: "*Our data show that between 4 and 6 million votes were lost in the 2000 election.*" Jefferson et al. [Je04, p.11] report: "*A recent example [of election fraud] involved boxes of paper ballots that were found floating in San Francisco Bay in November, 2001.*"

These incidents alone strongly motivate the discussion of the use of Internet voting systems and their ability to successfully address election fraud. Furthermore, supporters of these systems argue that there will be a higher voter turnout and more trust in elections. But unfortunately, using the Internet with its current architecture and protocols would cause more security trouble than we can handle.

The paper is about this trouble and the Internet's inappropriateness for remote voting scenarios. Section 2 shows the differences to e-commerce systems and discusses security aspects concerning the voting clients, voting servers, and the network connections between them from a theoretical point of view. Supplementary, section 3 summarizes Internet voting reports of some of the most important projects and links these experiences to the insights gained in sec. 2. Finally, conclusions are drawn in sec. 4.

2 Security problems

Security issues of Internet voting systems can be discussed from many points of views, e.g. technology driven, political science driven, or judicial driven. I address this field with a technology view, focussing especially on voting servers, voting clients, and the network infrastructure enabling the client-server-connections.

2.1 Differences to e-Commerce

Sometimes it is assumed by mistake that safely conducting commercial transactions over the Internet with SSL and server-side certificates means that one can also safely vote online using the same mechanisms. However, this is wrong, as Internet voting is different in many aspects [Je04]:

- Elections are inseparably linked to democracy and malfunctioning election processes can directly and decisively influence it. Democracy relies on broad confidence in the integrity of elections. Consequently, Internet voting requires a higher security level than e-Commerce does.

- It is not a security failure if your spouse uses your credit card with your consent, but the right to vote is usually[1] not transferable.

- A denial-of-service (DoS) attack might occur and prevent you and others from performing e-Commerce transactions. But generally there is a broad time window and after detecting and fixing the DoS attack business can be transacted. In the context of Internet elections a DoS attack can result in irreversible voter disenfranchisement and the legitimacy of the entire election might be compromised. For example, voters who want to cast their ballot during the last minutes of the voting time window would have no other voting channel available.

- Business transactions require your authentication by sending passwords, PINs, or biometric data. Voting however, requires authentication only when you register for an election and when you cast your ballot due to autorization, but concurrently demands anonymity to the vote (decision). This implies the adoption of much more complex security protocols.

---

[1] Exceptions must be allowed for blind and other handicapped people.

People can detect errors in their e-Commerce transactions as they have audit trails: they can check bills and receipts and when a problem appears recovery is possible through refunds, insurance, or legal action. Vote receipts (showing the vote decision and proving that the vote was unalteredly counted) must not be made out, as otherwise votes can be paid and extortion might occur.

2.2 Assumptions and focus

I consider only those voting scenarios whose voting protocols base on public-key-cryptography, certificates, and a public key infrastructure without addressing the protocols itself detailed, but this is no strong constraint. Furthermore I assume the potential voters to use ordinary PCs with Windows or Linux software and an arbitrary connection to the Internet.

Technological security issues are to be found in several dimensions (see figure 1, for a more detailed discussion see [Sch04]), but below I focus on hardware, software, and infrastructure as some of the most critical issues from my point of view. Voting protocols aren't less important but are basically out of range of this article.

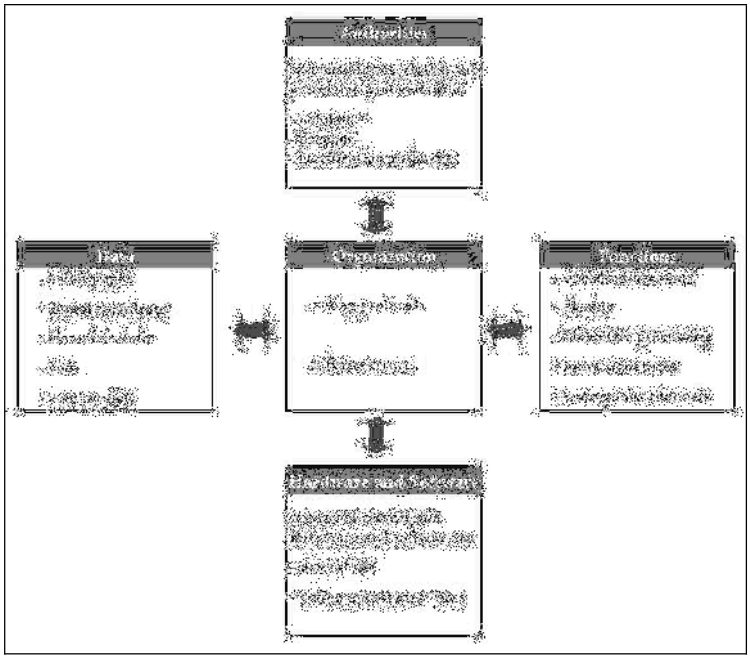


Figure 2: Security dimensions for voting systems [Sch04, p.7]

The following subsections address security issues of the client, the (voting) servers, and the connections between clients and servers. In particular I look at the voting process itself as opposed to online voter registration, which is a separate, but important and difficult problem.

2.3 Client related security issues

One of the most significant problems clients are facing is malicious payload (programs and configurations). Rubin [Rub02] analyzes this problem: There is virtually no limit to the damage viruses, Trojan horses, sniffing programs, etc. can cause. Although the presence of security defense software (virus and intrusion detection) becomes more and more widespread the current state of the art does often not go much beyond comparing a program against a list of signatures. If the security software vendor hasn't updated his definition files due to unknown signatures e.g., then a computer might remain unprotected for a while including the voting window. The option that the malicious payload and its signature will not be detected makes it all even worse. Using trusted software in the sense of signing software by a trustworthy entity and checking the digital signature of programs sounds like a sustainable concept, but this means that each piece of software has to be signed and checked. First, there is no software or hardware architecture supporting this, and secondly, Jefferson et al. [Je04] report cases where people were tricking Microsoft into signing a malicious ActiveX control. Summing up today there is no foolproof test for weather or not malicious payload is installed.

Rubin [Rub02] mentions the software Back Orifice 2000 (BO2K) that is freely available and fully open source tool for remote control of a computer. Once it is installed on a machine, it enables a remote administrator (or attacker) to view and control everything on that machine. As it is open source, an attacker might change the code so that is remains undetected by security defense software (due to a new signature). As it runs in stealth mode even a sophisticated administrator would have difficulties to detect it. Voting decision could be read, changed, and blocked from being sent without discovery.

As election dates are known in advance the activation of malicious software can be effectively triggered. The Chernobyl virus for example was scheduled for April 26, 1999, and affected many computers by modifying the BIOS in such a way that they couldn't even boot. If that happens on the day of an election many eligible voters would be disenfranchised. Politically ambitious attackers could target a particular demographic group aiming at a direct effect on the election's result.

And even worse it does not take a very sophisticated malicious payload to disrupt an election, as easy web browser attacks demonstrate. Most common browsers come with an option for a proxy setting that indicate that all web communications should take place via a proxy; the proxy is interposed between the (web) client and the (web) server and completely controls all Web traffic between these two. The proxy option can be easily changed by just adding a few lines to the preference file. Using the Netscape browser you just change the file prefs.js by adding these lines indicating that all web traffic goes to the corresponding server and port:

```
user_pref("network.proxy.http", www.malory.com);

user_pref ("network.proxy.http_port", 1799);
```

Although proxies cannot be used to read information in a secure connection, they can be used to spoof a user into a secure connection with the attacker, instead of the actual voting server.

Unfortunately, there are many ways for attackers to attach malicious payload to common PCs, most of us have probably experienced at least one option.

- Malicious payload can be installed by having physical access to the computer. Administrators in companies have full privileges on many computers and can infect them using setup routines on floppy disks and CDs. Many more scenarios are possible granting full physical access to an attacker.

- Most common malicious code is distributed via emails. Think about Melissa, I Love You, Sobig.F, and MyDoom/Novarg which infected probably millions of computers in a very short time. You don't even have to open an email attachment to get infected, e.g. the virus Bubbleboy was triggered as soon as a message was previewed in the Microsoft Outlook mailer. We can observe an alarmingly increasing activity.

- Buffer overflows are a known and well used point of attack. This kind of attack occurs when a process assigns more data to a memory location than was expected by the programmer. Web server programs and web browsers have proved to be susceptible for buffer overflows when arbitrary attacker's code can be executed. Buffer overflows are one of the most common form of security flaws in deployed systems today.

- A widely accepted but also dangerous way of executing programs is the use of ActiveX controls which are native code residing on the web server and attached to web content. If your browser's settings allow ActiveX controls to be executed they are automatically and maybe unknowingly downloaded and started. Trojan horses can be installed that way and on day of election brought to attacking execution. Many people use ActiveX controls as browser plug-ins, screen savers, calendars, etc., consciously or not. ActiveX controls can perform as man in the middle. This attack together with spoofing is addressed in the next subsection.

- Vendors of widely spread software like graphic programs, word processing program, etc. are in a strong position to change software and configuration files while the setup process is running. On day of election the changes can compromise or bother the voting process on this machine. Just let one rogue programmer of the software vendor be interested in subverting an election.

Authentication in the context of a public key infrastructure is done by signing data with the private key. Assumed the voter has a private key it must not be stored on the hard disk, floppy disk, CD, or USB stick, but should be kept on a secure key store like a smart card. As smart card readers are not directly connected to voting servers (voting) data flow through the insecure PC environment where it can be changed or blocked. Blocking of votes is easy: malicious code ensures that the vote gets not forwarded to the voting server.

Changing the vote is possible when you actually sign other data than you intended to sign: While your computer's display makes you believe you sign your vote for party A the malicious code changes your vote in favor of party B and sends this to the card reader. If this reader has no dedicated display allowing to double-check the vote then the voter might be fooled. The attacker doesn't even have to know your private key. Consequently, card readers without a(n) (expensive) display are insecure in this sense. Most voting systems don't even integrate any kind of card readers as they are not widely spread.

Today, mobile devices as voting clients drop out [IPI01, p.16]. Beside technical security problems displays are still limited in terms of display area, color, and resolution, as well as text input capability. They may easily be lost or stolen, and the cost for providing these devices to registered voters could be prohibitive.

Rubin [Rub02] sums it up: "In current public elections, the polling site undergoes careful scrunity. Any change to the process is audited carefully, and on election day, representatives from all of the major parties are present to make sure that the integrity of the process is maintained. This is in sharp contrast to holding an election that allows people to cast their votes from a computer full of insecure software that is under the direct control of several dozen software and hardware vendors and run by users who download programs from the Internet, over a network that is known to be vulnerable to total shutdown at any moment."

2.4 Server related security issues

The problem of DDOS attacks affects all participating servers. In this section we focus on the voting servers but generally the considerations can be applied to all servers. Attacks where legitimate users are prevented from using a system by malicious activity, are known as denial-of-service-attacks (DOS attacks). If many attacking machines collaborate to mount a joint attack on the target machine we talk about a distributed DOS attack (DDOS attack). In this scenario, an attacker could take control of many computers (called "zombies" or "slaves") in advance by spreading a virus or worm, and the slaves are waiting for instructions of a master computer to blindly follow them. There are mainly two forms of (D)DOS attacks: (1) The adversaries swamp the network connection of the targeted server with junk data that clogs up the network and prevents other, legitimate traffic from getting through. The SYN flood attack that exploits a weakness of the Internet protocol TCP is a famous example. (2) The adversaries are able to overload the server's computational resources with useless tasks that keep it busy. SSL-protected websites are susceptible to this kind of(D)DOS attack as the SSL protocol requires the recipient to perform a slow cryptographic operation (typically an RSA private-key computation).

Suffering a DDOS attack voting servers are in danger of being cut off from the Internet and eligible voters resulting in their disenfranchisement. If DDOS attacks are targeted demographically (regional voting server is attacked) and we have a close voting campaign then they could sway the election. DDOS attacks are huge and real problems and no effective protection mechanism is known.

Many DDOS attacks have occurred, an example of an DDOS attack on domain name servers is reported in the following subsection.

Another (easier) way to target a machine and to make it crashing is the *ping of death attack* [Rub02].

If voting clients would act as DRE (direct recording electronic) voting systems they wouldn't suffer from (D)DOS attacks as they could store the vote and send it later. Unfortunately, this approach seems currently not feasible, because it is not practical or desirable for PCs to emulate all the characteristics of DRE systems[2] [IPI01].

2.5 Connection related security issues

The sore spot of connection related attacks is the fixed election time window. Attackers can focus the last hours of the election window and paralyze the network of a region that is assumed to vote for candidate A by the majority. Even a quick fixing can take some hours resulting in the disenfranchisement of voters and affecting the election's result. One form of attack affects the Internet's Domain Name Service (DNS). The DNS is used to maintain a mapping from IP addresses, which computers use to reference each other (e.g. 134.130.176.7) to domain names, which people use to reference computers (e.g. www.winfor.rwth-aachen.de). The DNS is known to be vulnerable to attacks. Currently, there are just 13 DNS root server, some big companies additionally mirror them. In 2002 the DNS servers were exposed to a distributed denial-of-service-attack (DDOS) where several servers were fully loaded.[3] If on election day the DNS servers aren't available for many voters, then a connection to the vote server is not possible. Only those voters who know the IP address of their voting server could vote then.

Another attack is DNS spoofing where the true IP address of a domain name is overwritten with a fake IP address. The control of DNS root servers might be difficult, but the heavy use of DNS caching (on local or regional servers due to speeding up) makes this impossible. Although answering this problem with the protocol DNSSec (RFC 2535 und 2931) would be effective, its practical impact is low. Facing DNS spoofing the voter follows the instruction for voting and enters the denoted domain name. But unknowingly he gets a wrong IP address and he is spoofed into a communication with an attacker. He might receive a page that looks like the voting page.

Then the attacker acts as man in the middle giving him the power to abolish votes. The same happens in the context of social engineering: an attacker sends emails to voters containing links to the attacker's computer. When they look authentic many people would trust this email. Theoretically, this kind of spoofing can be effectively addressed with digital certificates of web sites, but today most people are not familiar at all with SSL connections and certificates and hence wouldn't check or discover this fraud.

---

[2] For more information about DRE systems visit http://www.verifiedvoting.org/drefaq.asp.
[3] http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A828-2002Oct22&notFound=true

Similar attacks could also work against the registration process. Eligible voters could be let to believe that they registered successfully, when in fact they were communicating directly with the adversary and not interacting with the legitimate registration server. The voters would discover when attempting to vote they were not registered. This could exclude them from voting.

Not to forget are attacks on Internet router which forward IP packets through the Internet to the server and back. If IP routers fail due to DDOS attack a whole region might be unable to cast votes.

Some attacks could be mitigated with the existence of a vote receipt proving that your vote arrived. As this receipt must not contain the vote decision[4] (see discussion above) itself it just proves that a vote decision arrived. There is no guarantee of data integrity, i.e. your vote could have been changed on your computer, on a computer in the network, or on the voting server. Many DRE (direct recording electronic) voting systems don't have any sort of voter-verified audit trail. Furthermore, how can you be sure that your vote was actually counted and not left behind? Traditional elections don't feature this problem as the whole process can be peered (except for absentee balloting).

3 Internet Voting Reports

Some projects have been set up to scrutinize the appropriateness of the Internet for a remote voting system. The most important ones are the *Voting Technology Project* of CALTECH and MIT [CM01], *A Report on the Feasibility of Internet Voting* of the California Internet Voting Task Force [CV00], *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)* [Je04], the *National Workshop on Internet Voting* of the Internet Policy Institute [IPI01], and *i-vote* of the Research Group Internet Voting [IV02].

Most projects come (after a detailed security discussion) to the conclusion that today the Internet should not be used for remote voting as the architecture, protocols, hardware, and software feature many vulnerabilities that could easily allow attackers to compromise elections. Only the German study [IV02] looks a bit more optimistical on Internet elections. Two projects [CV00; IPI01] distinguish between several stages of Internet voting and concede practicability for supervised Internet voting clients. The following subsections summarize the results of the corresponding reports.

[4] The Internet Policy Institute [4, p.19] discusses an approach that provides voters with the ability to vote multiple times, and have only the last vote count. However, some practical problems arise and make this concept difficult to be implemented.

3.1 CALTECH and MIT: Voting Technology Project

The CALTECH/MIT Voting Technology Project was initiated academically and conducted cy the California Instituite of Technology and the Massachusetts Institute of Technology as an interdisciplinary approach. It is not restricted to Internet voting scenarios.

However, regarding Internet voting they find [CM01, p.15; 42]: *"However, Internet voting, in the judgment of many experts, is not ready for wide-scale use. There are three problems. First, there are concerns of coercion if Internet voting is done from remote locations, such as the voter's home computer. Second, large-scale fraud is more likely because it is easier to hack the entire system if it is on the Internet, than it is to coordinate many millions of voters voting at precincts or thousands of poll workers. Third, many people do not have computers at home or are sufficiently intimidated by computers that Internet voting (either from home or at the precinct) might create a further obstacle to voting for millions of voters. […] Delay Internet voting until suitable criteria for security are put in place."*

3.2 California Internet Voting Task Force: A Report on the Feasibility of Internet Voting

The California Internet Voting Task Force was convened by Secretary of State Bill Jones to study the feasibility of using the Internet to conduct elections in California.

They define four steps of Internet voting and propose an evolutionary approach where stages 1 and 2 feature a supervised use of an Internet voting machine and stage 3 and 4 integrate remote Internet voting: (1) Internet Voting at Voter's Polling Place, (2) Internet Voting at Any Polling Place, (3) Remote Internet Voting From County Computers or Kiosks, and (4) Remote Internet Voting from Any Internet Connection.

The opinion of the Task Force is [CV00, p.1f]: "*At this time, it would not be legally, practically or fiscally feasible to develop a comprehensive remote Internet voting system that would completely replace the current paper process used for voter registration, voting, and the collection of initiative, referendum and recall petition signatures. […] However, current technology would allow for the implementation of new voting systems that would allow voters to cast a ballot over the Internet from a computer at any one of a number of county-controlled polling places in a county. […] The success or failure of Internet voting in the near-term may well depend on the ability of computer programmer and election officials to design a system where the burden of the additional duties placed on voters does not outweigh the benefits derived from the increased flexibility provided by the Internet voting system*."

3.3 A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)

The SERVE voting system was built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program) [DoD01] and intended to be deployed in 2004 for U.S. citizens living overseas; participating states are Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington. In the meantime the Pentagon refused to deploy the system in 2004 due to strong security concerns [DoD04]. A heavy security discussion was triggered by the security analysis report conducted by independent scientists. They disclosed they the SERVE voting system suffers from most security risks discussed above, stating [Je04, p. 3]: "*Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear."*

Surprisingly, without any security discussion it was announced that overseas voters can still vote by fax [DoD04].

3.4 Internet Policy Institute: National Workshop on Internet Voting: Issues and Research Agenda

The National Workshop on Internet Voting was funded by the National Science Foundation (NSF) and conducted by the Internet Policy Institute and the University of Maryland. It was former President Clinton who requested the NSF to examine the feasibility of online (Internet) voting.

Internet voting systems are grouped into poll site systems where voting machines are placed in traditional polling places, kiosk systems with voting machines located in convenient locations as malls, libraries, and schools, and remote systems where any computer that is Internet accessible might serve as a voting machine.

The core conclusion is [IPI01, p. 23]: "*Poll site Internet voting appears potentially able to meet currently accepted levels of risk; remote voting, however, does not, at least with current or soon available technology. The possibility of large-scale automated attacks on remote Internet voting systems leads to a level of risk so high as to be unacceptable."*

3.5 Research Group Internet Voting : i-vote

The German Research Group Internet Voting of the University Osnabrueck has conducted a project including the set-up of an Internet voting system and evaluating it empirically in the context of real elections. The report doesn't criticize remote Internet elections in principle, but argues more fuzzily claiming absolute secure voting clients, the certification of voting software and voting systems, and the use of chip cards with digital signatures. It admits, too, that much security research still has to be done.

4 Conclusions

Remote Internet voting heavily struggles with security issues and possible attacks that arise from the infrastructure, protocols, hardware, and software. There remain not only conceptual questions like how to deal with voting receipts and which voting protocol to use, but also everyday Internet problems like Trojan horses, viruses, spoofing, DDOS attacks, etc. Most reports clearly decline the appropriateness of today's Internet for remote elections. Two characteristics impose security stakes on a level we haven't faced before: (1) Remote Internet elections technically open a former closed voting environment to attackers all over the world who can gang together to selectively strike election processes. (2) The impact of a disrupted election can be large: the whole election might be questioned by an unsettled society and not less worse the election result might be notelessly effected. As our societies and states base on democracy and sound elections no described security risk is tolerable. According to Rivest [Riv01] adopting remote electronic voting means that we would have sacrificed too much security for the sake of voter convenience. However, the scale of security measures depends on the meaning of the election: voting a student parliament is not comparable with voting a national parliament that rules a state. Furthermore, supervised voting terminals and a closed Internet voting infrastructure don't feature many problems discussed above and are worth being more explored.

References

[CM01] California Institute of Technology (CALTECH) and Massachusetts Institute of Technology (MIT): Voting Technology Project, 2001. Available at http://www.vote.caltech.edu/

[CV00] California Internet Voting Task Force: A Report on the Feasibility of Internet Voting, 2000. Available at http://www.ss.ca.gov/executive/ivote.

[DoD01] US Department of Defense: Federal Voting Assistance Program, 2001. Available at http://www.fvap.gov/index.html.

[DoD04] US Department of Defense: Pentagon Decides Against Internet Voting This Year. American Forces Information Services News Article, Feb. 6, 2004. Available at http://www.defenselink.mil/news/Feb2004/n02062004_200402063.html.

[Je04] Jefferson, D.; Rubin, A.D.; Simons, B.; Wagner, D.: A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), 2004. Available at http://www.servesecurityreport.org.

[IPI01] Internet Policy Institute: Report of the National Workshop on Internet Voting: Issues and Research Agenda, 2001.

[IV02] Research Group Internet Voting: i-voteReport: Chancen, Möglichkeiten und Gefahren der Internetwahl. Zusammenfassung der Ergebnisse und Empfehlungen der Forschungsgruppe Internetwahlen zur Nutzung des Internets für Wahlen, 2002.

[Riv01] Rivest, R.: Electronic Voting, 2001. Available at http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf.

[Rub02] Rubin, A.: Security Considerations for Remote Electronic Voting over the Internet. Communications of the ACM 12 (45), pp. 39-44, 2002.

[Sch04] Schryen, G.: Security Aspects of Internet Voting. Proceedings of the 37th Hawaii International Conference on System Sciences, 2004. Available at http://csdl.computer.org/comp/proceedings/hicss/2004/2056/05/205650116b.pdf.

E-Voting and the architecture of virtual space

Anthoula Maidou, Hariton M. Polatoglou

Department of Architecture
Aristotle University of Thessaloniki
Gr 54124 Thessaloniki, GREECE
anthoula_maidou@yahoo.gr

Physics Department
Aristotle University of Thessaloniki
Gr 54124 Thessaloniki, GREECE
hariton@auth.gr

Abstract: One of the basic principles of architecture is that of the relation between function and form. It is a common fact that in most cases form reveals or refers to function. Thus by observing the form of a building one can envisage its function. Although the forms are different in different periods of history for reasons like the use of certain building materials and building methods, the specific socioeconomic conditions and the type of governance, one can find very few exceptions to the rule. The prevailing type of governance today is democracy and we are in a stage of dramatic change in the way people interact, get information and decide what to do concerning governance. This is mainly due to the revolutionary change in the communication, processing, representation and availability of information brought by the tremendous progress in the field of informatics. The representation is not restricted to some material form but it can take also an electronic form, existing in virtual space. Therefore there is great need for an architecture of the virtual space and even more important to establish a relation between form and function in the new environment. In this work we propose some principles and present some virtual space representations appropriate for e-democracy and e-voting.

1 Introduction

Since the early days of social organization, people had arranged various social functions in space and time and represented them by different forms. Houses had always different forms, than the places for public gatherings, for worship, for transportation, and for governance. This specialization is the result of the effort to represent function by form, since a building is much more than just a shelter - it is a bearer of ideas and symbols, reflecting the society that built it at the specific time. Of course, such form-function relation was constrained by the building materials, methods of construction, the external environment, and the social conscience, but Architecture had always expressed in built form the cosmological knowledge of each historical period [No96], at least until the nineteenth century. As the progress was slow historically, we could find only a small number of different representations of functions through form.

In the nineteenth century architecture could not express the edge of knowledge any longer. This was due to the invention of non-Euclidean geometry on the one hand, which could not be reproduced in built using the available building materials and techniques, and on the other hand was the reproducibility and ubiquity of books, which were much more powerful means of propagation of knowledge than architecture.

Presently we experience a revolution in the way we can communicate, process, access and represent information. This is due to the new information technologies. Storage devices enable the storing of huge amounts of data, accessible from everywhere around the globe. Digital representations, using virtual reality techniques, have led to the digitalization of architecture, offering a new experimentation field, free from materials, where new space-time reference systems can be applied. Marcos Novak, virtual architect and artist, introduced the word "transArchitecture" to describe current architecture, which has a twofold character: within cyberspace it exists as liquid architecture that is transmitted across the global information networks, while within physical space it exists as an invisible electronic double superimposed on our material world [No96]. Architecture has become transmissible, and thus is placed on a virtual shelf, available to be put to use on demand. Furthermore, form and function can be differently interrelated in virtual space. By changing the relation between form and function and decoupling reality from actuality, "we can vectorized significance into series of independent dimensions. We assemble what we need by picking and choosing among endless arrays of options" [Nov96]. transArchitecture establishes the lost connection between knowledge and architectonic exploration. "It brings knowledge … back into the realm of poietic experience" [No96].

Furthermore, the public places have lost their initial character as places for the exchange of ideas and communication [Mi95], while the internet and its easy accessibility, has given to everyone the ability to communicate his/her ideas with everyone else on the globe. The new communication technologies affect also the way political decisions are taken. E-voting is a new way of voting and is currently understood as a way to use computers at poll stations, to enable a correct and immediate election/poll result, or is considered as a novel way of voting remotely using the internet. Among the two types of e-voting the most promising and interesting seems the second one, although there are many problems to be solved concerning security issues, etc. E-voting through the internet is the most democratic way to let everyone take part at the decisions [KS03, SM03, TG03, WC02], since even older, ill or disabled people could take frequent and active part in the decision process. Although this is innovative, e-voting can and should offer much more than an opportunity to remote voting. It should offer information on the event, an agenda, on what is programmed to be tackled in the future, and direct democracy, where everyone can take part in the discussion and the decision. How and why this should be done will be analyzed in more detail below.

2 Method

In this work we have in mind e-voting with the use of the internet, when referring to this term.

2.1. e-voting environment: theoretical background

Current technological achievements enable the storing of enormous amounts of information and the access to it from everywhere on the globe. Nonetheless, it can cost endless hours to go through some of the available information, find the relevant topics and filter the information of interest to each subject. E-voting sites should be in action a sufficient time before the voting date, offering complete and detailed information on the subject in question. Furthermore, since information should be as representative as possible, everyone, citizen or organizations should have the opportunity to add his/her/their opinion on the subject at this site, and everyone should have access to all information, which should be stored in all possible formats, as texts, sound, picture, video format. It is reminiscent of the Ancient Agora, the market place of ancient Greek cities, but in addition the place for the exchange of views. Furthermore, everybody has to be able to be informed on all available opinions, either reading them or hearing them. Such a dynamic environment, where someone can also add an opinion could attract young voters. This is important in order to use the abilities new technology offers, namely direct democracy.

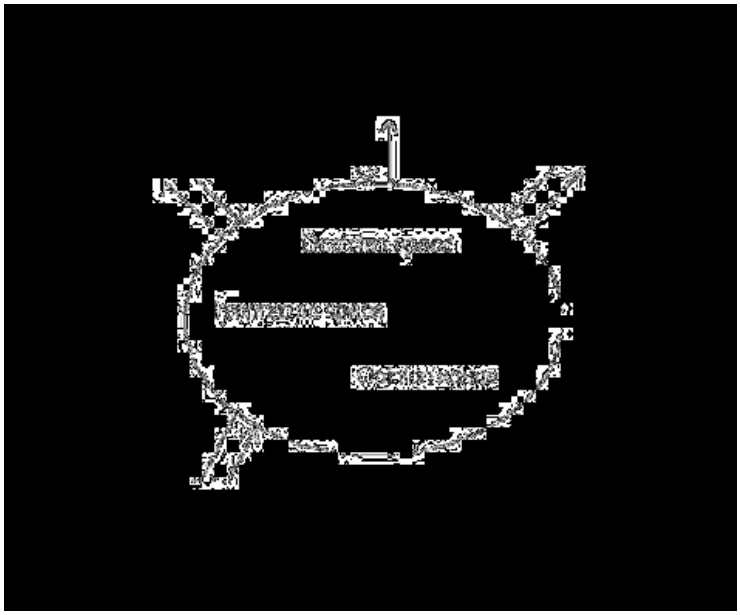


Figure 3: A many to many interaction of citizens with the decision process

In this way the scheme of the spaces/functions an e-voting site has to include can schematically be depicted in Figure 1. The information space is the place, where information can be gained. The opinion space is very important in order to obtain a democratic voting. Although it seems at a first glace that the “opinion space” could become too large to be useful, this is not the case, since on a specific subject only certain

distinguishable ideas can be expressed – if for example opinion A hasn't covered some matters, someone could add an opinion B to cover them, and so on. Finally, at the voting day, the voting place will also be accessible for the e-voting process, completing in this way the process of gathering information, exchanging information, and voting.

Furthermore, the authorities, that organize voting processes, should put on the web an agenda, where citizens can be informed on subjects to be discussed in the near future and be able to contribute to it.

2.3 Virtual space

The space we produce though the computer is virtual, it exist only as a digital representation, as a standing-reserve. It is immaterial. Furthermore, it doesn't obey physical laws, unless it is programmed to do. Neither do the restrictions we have as human beings, such as our dimensions and abilities apply necessarily to virtual space - we can "see" a large building form any height, walk through walls, jump from one place to another. Humankind has constructed a new kind of space.

The experience of a new kind of space isn't something novel. Since the implementation of the telegraph and later on the telephone and television, humankind is experiencing a new kind of perception, the "perception at a distance", or telesthesia [Mc94]. This experience is perceived as real, like the real world experience - it differs only in the fact that things are not bounded by the rules of proximity. Virtual space is also experienced as a real space - we use virtual space to get information on any subject, read the news, buy, visit libraries, museums, listen to music, etc. [Mi96]. Furthermore, the terms we use to refer to virtual space has a close analogy to the physical world: we talk about "virtual communities", "homepages" or "sites" that have "addresses", etc.

Virtual geographers study the geographies of the virtual space [DK01] using geographical metaphors. Additionally, we talk about the law of virtual space, protection of privacy, etc. Virtual space is perceived as a notional mechanism beyond the real world. Spatiality takes a new dimension; it can be electronically constructed and experienced. Through our memory we transform these experiences into possibly experienced realities. Virtual space is an extension of real space and can thus be analyzed in spatial terms.

2.2 E-voting interfaces

The main question we wanted to examine is how a successful human computer interface should be built, in order to attract people of various age groups, with a wide range of skills and abilities, and different degrees of voting experience, to take part at an election, or referendum. On the one hand we have special groups that are not familiar with the use of computers, and on the other we have the younger ages, which are familiar with computers, but show a minor interest in politics.

The question remains on how to communicate information, and how this information is correctly understood, in order for everyone to know what the voting is about, and also to give the impression of the importance this voting has. Originally, computers were designed by engineers for engineers – and little attention had to be paid to the interface. Later on, the use of computers by a broader, non-specialized user group necessitated the use of interfaces to enable them ease of use, correct understanding and interaction with the computer. The most important aspect in the Human Computer Interface design is to find efficient ways to design understandable electronic messages [No88, Sh98]. At this point we could take advantage of the achievements of virtual architecture.

In order to overcome these problems we propose that the appearance of the site should not be unique. As in electronic games, the visitors/citizens should be able to change the interface, choosing among various interfaces, in order to build their own environment, according to their taste. In this way people get familiarized with the voting environment.

A first step towards this direction should be the construction of more environments with various complexity and ease of use, which should be available to the visitor of the site, ranging from simple text sites, which should also be the default version of the site, to more complicate 3D graphics sites, to sites containing video and sound, or even navigable environments. At a second stage objects will be introduced, in a form similar to that of the avatars used in computer games, in order to invoke the feeling of their electronically projected self in this electronic environment, where interactions among the avatars (other visitors) could be possible. For example in the “Information Space” the various opinions could appear as avatars expressing their thoughts. A discussion group could also be organized as a place for the exchange of opinions. This could, in the future get the form of discussions among avatars. Such environments would specially invite the younger ages to take a look at the site, organize the interface according to their taste, get familiar with the structure of the site, and most important with the issue in question. In this way they will form an opinion, and probably take part at the e-voting process.

2.4 Virtual space

As to the interfaces and the navigation techniques, we used:

1.) A simple text and buttons interface in all spaces. Framed text displays the information, and links to the opinions, and the voting options. This is also the default interface.

2.) A 2d, or 3d graphics interface, which is used as a background. The actual interface remains about the same as in the first case.

3.) Video and interactive 3d graphics.

4.) Interactive navigable interfaces using VRML versions of the interfaces and graphical links.

3 Results

3.1 Presentation of some interfaces

Below we will give some examples. Because of the restricted space we will present only three interfaces. Of course, the acceptance of a virtual environment is not necessary – someone can also interact with the e-voting site using a default textual environment.

3.1.1 First example:

A scene reminding an ancient city market place serves as our first example. Picture 1 presents a part of it. In the center is a round temple, the tholos, with its altar formed as a multi-screen information place. It serves as the place, where information can be gained and also as the place for the exchange of opinions. Picture 2 shows a closer look at the information and opinion place. The upper section of the cylinder of the multi-screen contains the information space, while at the sides the opinions are displayed.

Picture 1: The first example displays an ancient marked (agora) interface. Here we present the part showing the "vouleftirion"(parliament) and the "tholos"(round temple).

Picture 2: The altar in the "Tholos" is a multiscreen projector. The altar plays the role of the information and opinion space.

Finally, at the voting date, the information and opinion space transforms into a voting-box, as presented in picture3.

Picture 3: At the e-voting day the altar transforms into a "kalpi" – a ballot-box.

3.1.2 Second example: a meeting room

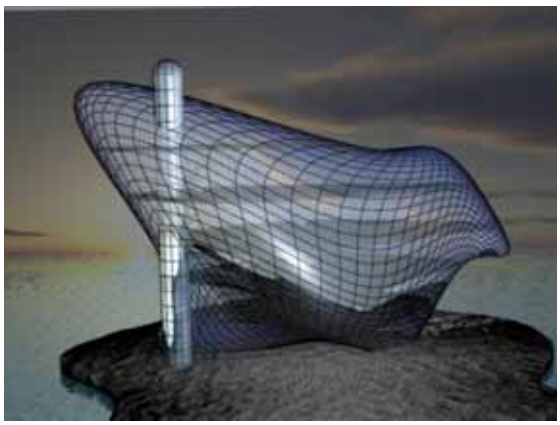
A large meeting table refers to discussion. The various opinions may be displayed as sheets of paper on the table, or as the human figures. Picture 4 presents such a room.

Picture 4: Second interface example, where the interface is a meeting room.

When it comes to voting the table transforms to a voting screen.

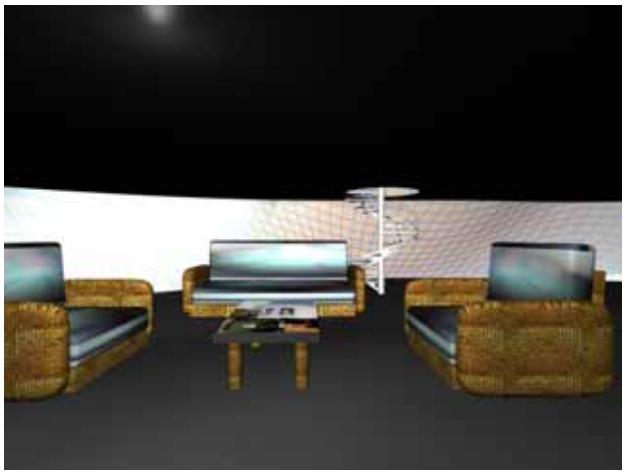
3.1.3 Third example:

Here the interface becomes an imaginary building, which refers to future environments.



Picture 5: The table of picture 1 transforms into an e-voting screen.

Someone enters the building and navigates in this VRML environment to gather information and express, read, or discuss opinions. An instance of how this could look is presented in picture 6.



Picture 6: An instance of the navigation in the information and opinion space

3.2 Testing results

We tested the interfaces on 16 persons, 9 women and 7 men, of various age groups1. With the help of a questionnaire, which was completed after the testing of the different interfaces, we found that both sexes and all age groups had no difficulty, at least after a short time they spend to get familiar with the interfaces. Some women and men of middle age group and all higher age groups participants preferred the simple text environment (about 35%) or the text and graphics interfaces (about 30%) and the video and graphics environment (about 35%), while the younger age groups were more attracted by the video and 3d graphics interface and the VRML navigate-able interface (about 50% for each).

In addition, more men (about 70%) were willing to spend more time reading different opinions, while a larger part of the women (about 65%) would prefer discussion groups.

Our findings showed that it is necessary to allow people to get familiar with the e-voting process through an earlier activation of the voting-site in the form of an information and opinion space.

---

[1] From the 9 women: 4 were under 30, 3 were between 30 and 55, and 2 over 55, while from the men 4 were under 30, 2 between 30 and 55, and 1 over 55.

Furthermore, about 60% of the younger age group admitted that they are in general not interested in politics and in community issues, but they would like to take part at e-voting processes, provided they could find objective information on the subject in question.

4 Conclusions

Current technological evolutions have changed the way we live, interact, communicate, learn, play get information, etc. Virtual reality techniques offer a new ground to architecture to take up expressing current knowledge and visualize data and information. The technological evolutions in accordance with the virtual reality techniques can be applied by governance in order to access the ideal of direct democracy. E-voting is the best way to allow citizens to express their opinion on major decisions of the political life of a community. Our findings showed that it is possible to attract younger voters, and encourage groups unfamiliar in the use of computers to participate.

References

[DK01] Dodge, M.; Kitchin R.: An Atlas of Cyberspace, Addison Wesley, 2001.

[KS03] Kampen, J.K.; Snijkers, K. : E-democracy - A critical evaluation of the ultimate e-dream. Social Science Computer Review. 21 (4): 491-496, 2003.

[Mc94] McKenzie, W.: Virtual Geography, Indiana University Press, 1994.

[Mi95] Mitchell, D.: The end of public space- Peoples Park, Definitions of the Public and Democracy, Annals of the Assosiation of American Geographers 85 (1): 108-133, 1995.

[Mi96] Mitchell, W.: City of Bits. MIT Press, 1996.

[No96] Novak M.: transArchitecture. 1996 http://www.mat.ucsb.edu/~marcos/Centrifuge_Site/MainFrameSet.html, as retrieved on 19.02.2004.

[No88] Norman, D.: The design of everyday things. New York: Doubleday, 1988.

[Sh98] Shneiderman, B.: Designing the user interface: Strategies for effective human-computer interaction (3rd ed.). Addison-Wesley Publishing, Reading, 1998.

[SM03] Smith, E.,; Macintosh, A.: E-voting: Powerful symbol of E-democracy. Electronic Government, Proceedings Lecture Notes in Computer Science, 2003, 2739: 240-245.

[TG03] Tambouris, E.,; Gorilas, S.: Evaluation of an e-democracy platform for European cities. Electronic Government, Proceedings Lecture Notes in Computer Science, 2003, 2739: 43-48.

[WC02] Watson, A,; Cordonnier, V.: Voting in the new millennium: eVoting holds the prondse to expand citizen choice, Electronic Government, Proceedings Lecture Notes in Computer Science, 2002, 2456: 234-239.

The UK deployment of the e-electoral register

Alexandros Xenakis and Prof. Ann Macintosh

International Teledemocracy Centre
Napier University
10, Colinton Rd,
EH10 5DT, Edinburgh, UNITED KINGDOM
a.xenakis@napier.ac.uk
a.macintosh@napier.ac.uk

Abstract: In this paper we analyse the experience gained in the 2002 and 2003 UK e-voting pilots in the implementation of the e-electoral register of voters. After theoretically establishing the need for an e-register, based on the analysis of the evaluation reports provided and direct observation undertaken in one of the pilots, we describe the systems used and identify the different organisational and technical issues that arose. Accordingly we highlight lessons learned, to be used for future implementations of the e-register.

1 Introduction

In August 2002 the UK government issued a consultation paper on a policy for electronic democracy [HM02]. This consultation document usefully argued that e-democracy could be divided into two distinct areas - one addressing e-participation and the other addressing e-voting. In the case of the latter the paper argues that e-voting should be viewed as a technological problem. In the case of the former, the document set out the possibilities for greater opportunity for consultation and dialogue between government and citizens. With regard to e-voting 16 pilots took place in May 2002 [Pr02] and 18 more in May 2003 [El03a], on a Local Authority level. These were in all cases legally binding elections. The different e-voting technologies piloted involved electronic counting schemes (in some cases combined with traditional paper ballots) touch-screen voting kiosks, internet voting, phone (touch tone) voting and SMS text message voting in 2002 [Pr02]. Digital television voting and smart card technology for partial voter identification were additionally introduced in 2003 [El03a]. Several local authorities (4 in 2002 and 13 in 2003) offered these technologies as alternative channels of voting, therefore providing a multiple channel e-voting process. In the pilots where two or more channels of voting were offered simultaneously an electronic on-line version of the electoral register was developed and used to provide the necessary infrastructure. The on-line electoral register was piloted in Liverpool and Sheffield in 2002, [El02a & 02b] and in Sheffield and St Albans in 2003 [El03b & 03c]. The focus of this paper is the analysis of the deployment and use of the e-electoral register.

2 Research methodology

The research presented in this paper forms part of a doctoral programme concerned with the identification of the emerging constraints in re-designing the electoral process in relation to ICTs. After completing an extensive literature review of the issues involved in the implementation of electronic voting, we have proceeded to the analysis of the detailed evaluation reports of the 2002 and 2003 UK e-voting pilots, provided by the Electoral Commission. Further research data have been provided directly by some of the 2003 pilot Local Authorities. Our research findings reported here on the e-electoral register are based on its use in one of the 2003 pilots. The Local Authority studied was piloting an on-line system of the electoral register, to support a simultaneous multiple channel e-voting process combined to provide e-enabled polling station voting. The fieldwork which comprised interviews and observations, was conducted both during the run-up to the election and on the actual polling day. Semi-structured interviews with Local Authority and commercial suppliers' staff were undertaken on the first day, during which, there were interruptions to allow for managerial problems to be resolved. In such cases the observer was allowed to follow the e-voting management in action. On election day, observation took place at the operations management centre, which was set up to handle the technical and organisational issues that arose. After 9pm that day, when voting was over, the observer was part of the verification processing team. That in turn provided the opportunity to acquire hands on experience of the administration of the e-register system used.

3 The need for the e-register of electors

The Electoral Commission in a report specific to the electoral registration process [El03d, p:18] recommends: "Electoral registers should be universally electronically maintained according to mandatory national data standards". It also refers to issues concerning registration fraud and measures that could be taken to prevent against such fraud. In the previously mentioned UK Government consultation paper, a system described as: "a local or national electronic electoral roll" p43 is suggested as necessary infrastructure for voting at any polling station. Also, the on-line electoral register is considered to be one of the major components of a modern e-voting system, along with "on-line registration and application for postal votes, on-line and text voting, e-counting and collating of election results" p45. The major benefit given for a central electronic electoral register is that election officials could authenticate a voter at any polling station. Research in this area has been undertaken by the LASER (http://www.idea-infoage.gov.uk/services/laser/index.shtml) project aiming at the production of a fully interactive online register. The need for the e-electoral register serves the basic security requirements that "only people who are entitled to vote can vote" and "nobody can vote twice or in another person's name (unless an authorized proxy)" [HM02, p46].

From a legal point of view voter identification is necessary in order to avoid personation [Xe03]. The Watt [Wa02] report defines the different cases of personation, while making the case for the legal requirement of 'one ballot per vote' and a verifiable count.

Furthermore, who is included in the electoral register is directly related to the issue of voter eligibility [OS01]. In accordance with the above, the statement of requirements for the design of the e-voting systems to be used in the 2003 pilots included a "Compliance with Legislation" term [OD02]. Technical security standards were also set according to CESG security solution [Cr02]. Managerial issues were also covered in the 2003 statement of requirements, including data management, risk management and staff training. The same set of requirements had a separate section for the electoral roll with several detailed functions that had to be developed by the suppliers and provided to Local Authorities. The most relevant functions with regard to this paper covered the necessity to convert any electoral roll into a format which is suitable for use in the pilots, immediately mark an elector as having voted as soon as the ballot is counted, provide upon request a daily marked register and allow a live continually updated register to be accessed remotely by the Returning Officer or the Local Authority staff.

4 Issues in the 2002 pilots

In the Sheffield 2002 pilot [El02b] three e-voting channels were simultaneously offered (internet, SMS text and kiosk voting) for a period of 6 days leading up to election day, along with voting in polling stations on election day. The existence of the on-line e-register enabled voters to cast a ballot at any polling station within their ward. Three wards out of twenty-nine were participating in the pilot. The voting channels provided in the Liverpool 2002 [El02a] pilot were similar to the Sheffield pilot with the only difference being providing telephone voting instead of kiosk voting. These were offered for the same period of time but only in two wards out of thirty-three. The e-register used a VRN (voter reference number) as a unique elector identifier, which was consumed once an e-channel had been used. That excluded double voting between e-channels. On election day a voter who requested a ballot from a polling station, was checked against the on-line e-register during the identification process. That excluded the possibility of a voter having already voted at another polling station or doing so later in the day. Polling officials by marking the e-register when giving a ballot would automatically consume the e-credentials of the voter and exclude the possibility of double voting between polling stations and e-channels. If a voter had previously applied for a postal vote then their e-credentials would also be consumed. In Sheffield a voter could go to any polling station of the participating wards and tell their name to the polling official. The polling official would in turn look the voter's VRN on a paper-printed list and input in the e-register interface. This made the process more time consuming than the traditional crossing off on the paper register. In Liverpool the same process was followed, but as an extra element of procedural security, voters were also crossed off a paper version of the register as would be done in the traditional voting process. This made the authentication process even more time consuming, about thirty seconds per voter, instead of five seconds needed had the traditional process being used. This, in turn, resulted in long queues building up during the evening.

4.1 Organisational Issues

A consortium made out of two commercial e-voting providers delivered both pilots. In Liverpool however a third commercial provider was involved in supporting the pilot effort (voter call centre). In Sheffield two PA departments were involved in the project (election office and IT) while in Liverpool four PA departments were involved (election office, e-government, marketing, press office), with the traditional voting channel managed separately. In both cases the project was lead by the main commercial supplier and there was a great amount of trust and dependence of the PA on the commercial suppliers due to time constrains in delivering the project. Risk management was adopted based on thirteen high-level risks, which were eventually detailed in late April –the election day was 2nd May. The 2002 risk tables were not provided in the 2002 evaluation reports. Polling station staff training was limited; in Sheffield one hour in the use of the register was provided prior to election day along with an instruction manual. In Liverpool two hours of un-paid training were provided but there was no time for process simulation. Limited staff training was considered to be an additional reason, which caused delays in the authentication process and also the reason for some of the technical problems encountered.

4.2 Technical Issues

Laptops and ISDN lines were used to connect polling stations to the on-line e-register. In Sheffield, there were also some cases of polling staff having difficulties in setting up the laptops, however a help-line provided assistance to polling station staff. Overall, only 4 cases were reported of voters being denied the right to a ballot as the e-register recorded them as having already voted. All these cases were attributed to processing errors. To cover the risk of hardware failure, contingency plans included one technician with a spare laptop per ward on polling day. To cover the risk of temporary system failure, provisions for keeping paper records of those who had voted at polling stations were taken for later entry once the system was restored. If the system was however permanently down then provisions were taken to convert immediately to traditional elections without the option of voting at any polling station. In Liverpool similar contingency planning was in place. ISDN connection problems were reported in two cases and were attributed to poor staff training; apparently polling station staff had damaged the equipment provided in their effort to install it. Technical support was provided to rectify the problems with backup hardware. In another case, a polling station received the wrong laptop. The polling clerk did not follow the agreed contingency procedure (telephone the central office and verify the eligibility of each elector) and for two hours issued ballot papers keeping manual notes of the voters who had been given a ballot only to update the database once the problem had been restored. Although all voters were later proved to have been eligible for the ballot they had received, there was a clear possibility for them to double vote during that time through another voting channel. The 2002 Liverpool pilot indicated that human errors could lead to technical risks and procedural disruptions. Had the lesson been learned for this case, problems might have been prevented in the 2003 pilots involving the use of the e-register.

5 Issues in the 2003 pilots

In the May 2003 elections St Albans [El03c] provided a multiple channel e-voting process including touch-tone telephone, kiosk and internet voting for a period of three days leading up to election day, along with simultaneous voting in polling stations on election day. The existence of the online e-register enabled voters to cast a ballot at any polling station as all twenty wards and twelve parishes were involved in the pilot. Additionally SMS text voting was offered in Sheffield [El03b], along with smart cards, which were used to facilitate the authentication process at polling stations and kiosks. The Sheffield 2003 pilot lasted for a voting period of seven days, with election day being the last one, however only fifteen out of twenty-nine wards participated in the pilots. The e-register system used in both pilots was the same as the commercial supplier provided it. The system provided seven functions: voter search, marking the register, credential management authentication, issue of replacement credentials, issue of tender credentials, checking the contest history of a voter and viewing an audit log for each voter.

In both cases laptops were necessary in order to maintain and update the electronic version of the electoral register in real-time from each polling station. This was necessary to avoid double voting as any voter could, up to the last moment (9pm on election day), cast a ballot through any of the voting channels offered. In practical terms this means that if a voter cast a ballot via a kiosk and then attempted to vote in person at a polling station the polling official equipped with a laptop connected to the database of electors (e-register) through the internet, would know that this voter had already cast a ballot and would subsequently deny a second ballot to this voter. More importantly, as voters were offered the option of voting at any polling station in all wards experimenting with the use of the electoral register on election day, the updated e-register would prevent a voter from voting at more than one polling station.

In Sheffield laptops were also used in polling stations to introduce an innovation at the authentication process. Each laptop was connected to an external smart card reader and voters were provided with the option of bringing their smart card to the polling station. The smart card could be used by the voter in front of the polling official and once passed over the smart card reader (non-contact smart card technology was used) the voter's details would automatically be recalled from the on-line e-register. The polling official would then ask the voter their name and address to verify against the screen information from the e-register database, and in this way complete the authentication of the voter. This should have been a 10 seconds process for each voter. The aim of the smart card was therefore to produce time efficiency in the polling station voting process. The smart card's memory element contained the voter identification number. It could also be used in kiosks. Once inserted in the smart card reader of the kiosk the voter ID would appear on the screen and voters would only have to supply the system with their password. However in all cases the use of the smart card was optional. At a polling station a voter could just walk in, state one's name and address, then the polling official, using function one, enter these details and authenticate the voter looking at the e-version of the register rather than the paper version of the register.

This was supposed to be a 30 seconds process and such was the case in St Albans where no smart card was introduced. Similarly at a kiosk a voter could type in one's voter ID instead of inserting one's card in the smart card reader. In all cases the smart card did not contribute any extra element of security but was rather provided as a means of convenience.

5.1 Organisational issues

A total of eight commercial suppliers had to work together to provide the Sheffield pilot [El03b], while the PA contributed with the election office, and staff from the IT department and the office of the Returning Officer. In St Albans [El03c] seven commercial suppliers were involved and the PA contributed with the IT department and a dedicated e-voting working party. Commercial suppliers were either directly contracted or subcontracted by the main providers. The main suppliers were the same for both Local Authorities.

Following basic IS project management principles [Av03] one would expect contingency planning at least equivalent to the one identified in the 2002 pilots. The statement of requirements for the 2003 pilots [OD02] asked for the implementation of a methodology compatible with PRINCE2 [Be02]. St Albans PA did provide an approach consistent with PRINCE2 while Sheffield PA followed its own methodology. In both cases risks were managed as they arose. However the matter of reliance of the PA to commercial suppliers for the safe delivery of the pilot remained and was characterised as over-reliance by independent evaluators working for the ODPM [El03b].

With regard to polling station staff training, the evaluation reports indicate that a greater effort was undertaken than the previous year. St Albans provided a detailed training programme, while Sheffield provided a two-hour walkthrough of the system for at least two out of three polling clerks of each polling station. However trainees were not given the opportunity to browse the system prior to election day, and gain familiarity with the different features. Instead they were provided with and interactive CD and a detailed manual. For Sheffield in particular no training was provided on the connection of the smart card reader to the laptop.

The organisational problems that arose were similar in both pilots. In Sheffield [El03b], there were delays in the delivery of laptops and smart card readers, while the number of back-up systems proved to be insufficient. Laptops were incorrectly configured by the responsible subcontractor, who also provided half the promised technical support staff with no transport and no knowledge of the area. Polling stations were not provided with a back-up paper copy of the register, as was the case in the previous year. In St Albans [El03c], the hardware required at polling stations on the morning of election day, was installed but not operational (41%), delivered but not installed (43%), or in very few cases not even delivered (5%). According to the project plan polling stations would be equipped with the necessary hardware the day before election day or even very early in the morning of election day (5am-8am). The reason was the unavailability of dedicated locations to serve as polling stations, which posed time constraints as to when the installation could take place. The time and the resources needed to set up polling stations

were underestimated. Inadequate logistical planning resulted in engineers being sent to polling stations without local maps and site installation diagrams. In both cases there was concern about the internal communication between the main contactors and their subcontractors.

Organisational problems, along with the technical problems described in the following section, resulted in a significant number of polling stations not being connected to the e-register in the morning of election day. In Sheffield the back-up procedure was that polling officials would call the election office and the election office staff would enter the voter in the e-register. However election office staff was unavailable and hand written notes were kept by polling clerks on those voters who had been given a ballot. There was also a written instruction given out to polling officials asking them only to give a ballot paper to a voter when marked on the e- register and not before and if in doubt contact the election office. Following instructions some polling officials did not give out ballot papers and some voters were sent away advised to come back at a later time in the day or use an alternative voting channel. According to the Electoral Commission this resulted to 200 voters being sent away [El03b].

In Sheffield, the main source of confusion in managing problems derived from the fact that there was no provision for established channels of communication between the polling stations and the election office. In St Albans mobile phones were issued to polling station officials. Sheffield on the other hand relied on the provision of telephone lines at polling stations.

The solution suggested, to provide election officers with a paper copy of the register, would have to be a copy of all registered voters in all participating 15 wards. If such copies were not already available, they would have to be printed out and then delivered to the polling stations facing problems in the use of the electronic form of the register. The copy of the register provided to the polling stations in question would be marked with the voters who had already cast a ballot through a different voting channel during the previous days. Although this measure would not provide total security against possible election fraud, as voters could vote again and again at polling stations where there would be no form of real-time updated register, it would limit the possibility of fraud, as it would exclude those who had already voted from voting again. However, the suggested solution was not feasible because of the large number of polling stations reporting problems with the e-register. In contrast, St Albans did provide the polling stations facing problems with the e-register with marked paper copies of the electoral register early on election day [El03c], but these reflected the status of the register at one particular time (10.15am) and were not subsequently renewed later in the day.

In relation to the voting process, when smart card readers did work, then the process could also be delayed instead of expedited as expected. Voters did not know how to use the card because there was no voter education on that matter. The smart card used in Sheffield was of the latest technology and in effect that was the problem as the technology was so new that people had no user experience of it. It was a “proximity card”. A voter did not have to insert it in a slot, as would have been the case in using a kiosk or any automated cash dispenser. In effect the card was contact less and it had to

be passed slowly over the smart card reader. Typically voters would put the card on the reader or pass it over quickly and the reader would not recognise the voter ID contained in the card. More efforts were needed to get it right and as a result more time. The problem could have been limited had training on the use of the card been provided to the polling officials, who could then help voters effectively.

At the close of polls, all the polling stations, which had kept manual notes on the voters who had voted without being properly authenticated, returned these notes to the election office. Normally the notes would have the name, surname and street address of each voter. The verification process started at 9pm after the e-voting channels closed. The database would then be searched usually with one term (surname) and accordingly verified on screen in relevance to the rest of the data. If the voter was shown as not having voted then he/she would be marked and there was no problem. If the voter was shown as having already voted there were available audit trails providing information as to the channel this voter had used.

However this was a time critical procedure because the result could not be announced before this process was over and the possible damage done during the day (double voting) fully measured. There was no consistency in the form of notes provided by different polling stations. All of the notes were hand written which in some cases caused confusion as to what was written. The objective of the verification process was to check and mark the register as should have been done during the authentication process prior to granting a ballot. If the register were already marked that would mean that a vote had already been cast on an e-channel and that the paper vote should be counted as valid. The general rule in the multiple channel voting was that if double voting had indeed happened then the e-ballot would be ignored and the physical (paper) ballot counted. This rule would cover the case where someone had voted twice, once in a polling station and once in any of the e-channels. However the case of a voter casting a ballot in two or more polling station was not covered, as all these ballots would be paper ballots. The process followed is an example of a procedural security measure [Xe04] adopted to cover for a technical inefficiency.

5.2 Technical issues

Regarding internet connectivity, in some cases the e-register, would respond more slowly than expected. This could be attributed to any number of different reasons, for example, the database server being overloaded (performance degradation). In such cases manual notes were kept to enter later when the system performance allowed it. That mainly caused periodic crashes around the end of the day and it was attributed to data indexing problems at the bottleneck of the back-end application. ISP poor performance also resulted in a slower process by not transporting data at the expected internet speed. ISPs guarantee connection to the internet but not internet performance. Dedicated fixed connections or the use of an owned ISP was suggested as a future, nevertheless more expensive, solution.

Connectivity problems also included some polling stations loosing their connection from time to time. In cases where there were long periods of time between two voters coming to be identified the connection would automatically drop. This lack of continuous connectivity meant that polling officials would have to re-log on to the database when the next voter needed to be authenticated. On entering the database for the first time polling officials were prompted to change their password. In one similar case the polling official forgot the new password that he/she had provided and therefore could no longer gain access to the e-register.

In Sheffield, hardware problems were also reported in relation to the smart card readers. The smart card readers were an external element linked to the laptops with a cable connection but they had a different power supply, which proved fragile. Polling station staff had to take the laptop and the smart card reader out of their cases, place them on a table, link them in the appropriate way according to each different laptop make, and then plug-in both power supplies and start the computer. The problem was not the reader itself but the separate power supply provided for the readers. Nevertheless a defective smart card reader did not stop a polling station from accessing the on-line e-register, but only changed the way voter searches were done.

Finally, with regard to the risk of power cuts, which was discussed at length in the 2002 Electoral Commission evaluation reports, the use of UPS units was reported only in St Albans. Nevertheless, normally charged laptop batteries could have kept the polling station operational for about four hours.

6 Conclusions

An e-enabled election is made more difficult to deliver as the scalability of the project increases. The deployment of the e-register studied in this paper, highlights the following issues:

- There is a need to establish standard communication channels between all the agents involved in the delivery and management of the e-register. The provision of alternative networks of communication such as the use of mobiles in St Albans proved useful practice, which facilitate the management of the problems faced and the need for feedback and problem escalation mechanisms between the agents related in the delivery of the pilot.
- There is an obvious need for a co-ordinating agent when many different agents are involved in delivering intersecting e-voting processes.
- The type and quality of internet connection used and the well-organised technical support provided, will determine the time needed to authenticate voters.
- Backup procedures such as a paper version of the register must remain available before problems arise, at least until the new process is well established.

- Systematic staff training in the new methods of voting to a level of being able to provide on-sight voter education and process knowledge gathering can provide valuable input to future best practice.
- Problems in e-enabled voting, resulting in process risks are related to the one-off use of voting locations (polling station) for the purpose of voting and every extra piece of equipment used.

From a more generic point of view, loosing voters who would have voted if not prevented by malfunctions in the e-enabled electoral process, could become a major political issue when affecting larger number of voters. This fact could in turn undermine the validity of the result of the electoral process as a whole, even if only one of the voting channels were problematic. The lessons learned from the deployment of the e-register in the UK can serve as a set of valuable guidelines for the future design and deployment of e-voting systems.

References

[Av03] Avison, D.E. & Fitzgerald. G., Information Systems Development: Methodologies, Techniques and Tools, 3rd Edition, McGraw-Hill, Berkshire, (2003)

[Be02] Bentley, C., PRINCE2: A Practical Handbook, Butterworth-Heinemann, Oxford, (2002)

[El02a] Electoral Commission. Pilot scheme evaluation Liverpool City Council 2 May 2002

[El02b] Electoral Commission. Pilot scheme evaluation Sheffield City Council 2 May 2002

[El03a] Electoral Commission. Local electoral pilot schemes 2003, Briefing, April 2003

[El03b] Electoral Commission. Pilot scheme evaluation Sheffield City Council 1May 2003

[El03c] Electoral Commission. Pilot scheme evaluation St Albans City and District Council 1May 2003

[El03d] Electoral Commission, The electoral registration process, Report and recommendations, June 2003

[El03e] Electoral Commission. (2003e), Technical Report on the May 2003 Pilots

[HM02] HM Government. In the Service of Democracy - a consultation paper on a policy for electronic democracy. Published by the Office of the e-Envoy, Cabinet Office, London, (2002).

[OD02] ODPM, Electoral Modernisation Pilots, Statement of requirements, (2002)

[OS01] OSCE, Office for Democratic Institutions and Human Rights, Guidelines for reviewing a legal framework for elections, Warsaw, (2001)

[Pr02] Pratchett, L. " The implementation of electronic voting in the UK " LGA Publications, the Local Government Association, (2002)

[Cr02] The Crown, E-voting security study (2002)

[Wa02] Watt, B., Implementing Electronic Voting, A report addressing the legal issues by the implementation of electronic voting, University of Essex, (2002)

[Xe03] Xenakis, A. & Macintosh, A, A Taxonomy of Legal Accountabilities in the UK e-voting pilots. In proceedings of DEXA, E-GOV 2003, Springer, (2003)

[Xe04] Xenakis, A. and Macintosh. A., Procedural security in electronic voting, in the proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), (2004)

Transparency and e-Voting
Democratic vs. commercial interests

Margaret McGaley, Joe McCarthy

NUI Maynooth
Computer Science Department
Co. Kildare, IRELAND
mmcgaley@cs.may.ie

Arkaon Limited
Sandymount
Dublin 4, IRELAND
joe.mccarthy@arkaon.com

Abstract: Electronic voting systems are being introduced, and have been introduced, in many countries for a variety of reasons. The introduction of computers into the electoral process can offer several advantages. Among other things it can speed up the process of calculating results, can help voters avoid accidentally spoiling their vote, and can allow voters with special needs to vote in private. Often, however, little consideration is given to the potential negative effects of electronic voting. We examine some of these negative effects in terms of the three streams of this conference: technology, law, and politics, with particular emphasis on the situation in the Republic of Ireland. The over-arching theme of this paper is that the introduction of technology into the democratic process can reduce transparency, and risks private commercial interests being given priority over public democratic interests.

1 Technology

The introduction of technology is often seen as necessary to progress, and therefore in some way unstoppable. All too often, however, little consideration is given to the new challenges - legal, political and sociological - posed by technology.

1.1 Transparency

Perhaps the greatest strength of paper voting systems is their transparency. Individual voters can satisfy themselves that the system works, because its transparency allows them to observe and understand every aspect of it. Nothing within the system is secret or impenetrable, except of course who casts which vote.

Purely electronic systems cannot offer this transparency. The nature of computers is that their inner workings are secret. Since transactions and calculations happen at an

electronic level, it is not physically possible for humans to observe exactly what a computer is doing. Once the vote is cast the voter "loses sight" of it. So if - for whatever reason - the vote is stored incorrectly, there may be no sign that something went wrong.

The change from paper to electronic records is not simply a matter of changing the storage medium. It is much more fundamental: the introduction of a computer system between voter and vote denies the voter tangible evidence that his vote has been recorded correctly. This is different from the paper system. While the voter never received evidence that he could take home, he did see the actual record of his vote (the paper ballot). Armed with the knowledge that pencil lead does not fade overnight, he could then be sure that the vote cast would be the vote counted. When the primary record of one's vote is electronic, on the other hand, one only ever sees a representation of one's vote, never the vote itself.

It is unacceptable that a voter should have to trust any agent or device to correctly relate their vote to them. Unfortunately, this is necessarily the case with purely electronic systems.

1.2 Voter Verified Paper Ballots

There is growing support worldwide [U.S, Sch00, Soc04] for the idea that 'Voter Verified Paper Ballots' (VVPBs [Mer92], also known as a 'Voter Verified Audit Trail') must be a requirement for electronic voting systems. VVPBs are paper records of the vote which have been verified by the voter at the time of casting. They might be hand-written ballots which are scanned for computer counting, or they might be printed by DRE (Direct Recording Electronic) machines in front of the voter before being deposited into a sealed ballot box [Mer02]. These paper ballots, however they were produced, would be the primary record of votes cast, since they would be the records verified by the voter. They would be used for all recounts and in a number of randomly chosen constituencies every time the system was used.

Some manufacturers of electronic voting systems, including the Nedap system being introduced in Ireland, have suggested that printing all the ballots after the close of polls would provide an equivalent audit trail. In fact this would be completely inadequate. The value added by VVPBs is that they are a record that has been confirmed correct by individual voters. If, by accident or design, the electronic records were incorrect then printed copies of those records would contain the same errors. As the old computer phrase goes - garbage in, garbage out.

Several paperless alternatives are under development [Cha04, JRB03]. However, we have yet to be convinced that any such system can provide the transparency necessary, or release voters from having to trust vendors.

The elimination of paper from elections is a significant motivating factor in the introduction of electronic voting for many governments. However, because of the nature of electronic systems, the removal of paper from voting may never be compatible with trustworthy elections.

1.3 The Nedap/Powervote System

The machines to be used in Ireland in June 2004 are classed as DRE (Direct Recording Electronic). That is, votes are cast by inputting preferences to the machine and are recorded directly to storage media within the machine. They are not touch-screen as are the majority of DRE machines used in the USA. Instead, they present the voter with a panel of buttons on which a printed sheet indicates which candidate/option is represented by each button.

Votes are stored on "ballot modules", cigarette packet sized memory cartridges. At close of poll, the contents of the main module are copied onto a backup module which remains in the voting machine unless and until needed. The main ballot modules are collected from the various polling stations and brought to a constituency count centre (in pilots undertaken so far, they were taken by taxi [Fit02]).

At the count centre the modules are read into a desktop PC[1], where the IES (Integrated Election System) count software - written in Borland Delphi and using Microsoft Access - calculates the results. The main vulnerabilities to malicious attack and/or error identified by us so far are outlined in the table below:

Stage:	Vulnerable to:	
	Malice	Error
Development of hardware/software	✓	✓
Storage of machines between polls	✓	
Backup copy		✓
Transport of modules	✓	
Loading of votes from modules	✓	✓
Separation of ballot papers for counting (where multiple ballots are cast on the same day)	✓	✓
Counting results	✓	✓

Figure 1: Vulnerabilties

2 Law

The introduction of e-voting raises questions about the legal position of:

- the electoral rules
- the electoral results
- the vendors of the system

It is vital that the law moves to meet the new challenges posed by introducing new technology.

[1] The number of PCs involved at this stage and the nature of their interconnection is somewhat unclear [see Section 3.2]

2.1 Electoral Rules

The Irish Electoral Act [Ele92] 1992 laid out the rules by which votes should be counted in Irish elections. The act outlined the particular form of Proportional Representation - Single Transferable Vote (PR-STV) mandated in the Irish constitution, including the specific rules to be followed during counting. Thus the Irish Electoral system was completely described in law.

Since the introduction of enabling legislation for electronic voting in 2001, the rules for deciding Irish elections are no longer dictated solely by the relevant law. The software within the system is in fact the final arbiter. Under current agreements between the Irish government and Nedap/Powervote this leads to an extraordinary situation. The count rules no longer belong to the Irish people, are no longer public and are subject to change without legal procedures.

The Electoral Law has been interpreted by the Department in a document called the "Count Rules"[2]. This document serves as the user specification for the programmer. No other documentation exists except the application itself which is in some 150 to 200 modules of Borland Delphi code. The overall codebase is 200,000 lines of code originally established for use in the Netherlands. It has been modified for use in Germany, in Ireland and in the UK. It has recently been further modified for use in a trial in Brest, France. The reviewers' comments [NTec] indicate that there is no separation between the UK and the Irish code base for certain modules. This is a very dangerous practice since the electoral rules are completely different in the two countries - the UK uses "first past the post" whereas Ireland uses PR-STV.

2.2 Electoral Results

In the paper system, the law required that ballot papers be kept for a minimum period of six months in provision for disputes arising. In such cases, a court could require that the paper ballots be re-examined. A similar provision has been made within the electronic system, but as the only records of votes cast would be electronic, the only evidence which could be presented in court would be electronic evidence (or a printout of electronic evidence, which is of course no more reliable). It is difficult to have electronic evidence admitted in a court of law [Lam02] and rightly so, since it is so much more easily manipulated and tampered with.

The legal position of electronic ballots has not been tested in any Irish court, but the possibility that results could be successfully appealed on this basis should certainly be considered.

---

[2] Available for download from http://evoting.cs.may.ie/Documents/DoEHLGCountRules.doc

2.3 Vendors

Electronic voting systems are different from other software and hardware products, because of the vital role they play in the democracies where they are used. It makes sense therefore that the vendors of such products should be treated differently. The commercial interests of those companies cannot be allowed to take precedence over democratic interests.

Perhaps the most obvious conflict between these interests is in the matter of trade secrets. Normal practice within the software industry is for software developers to keep the source code for their products secret. The same applies to all the documentation produced during the development process, including design documents, and test strategies and results.

If the public is to be satisfied that the system was well developed and does what it is supposed to do, this documentation must be made publicly available, so that those with the skills to examine its quality have that opportunity. While this approach prioritises public interests over private, it is not all negative for the company. There are many successful businesses today that use the open source model. For example, the Australian electronic voting system was produced by a commercial company, and its source code is available for download [Aus]. This has already resulted in several flaws being discovered and corrected [Zet03].

A further conflict of interest is this: if there is a flaw in the system it is very much in the public interest that such a flaw be discovered and corrected. This would be bad publicity for the vendor, however. Unfortunately it is not safe to assume that a business will put the correct working of democracy ahead of its own reputation. Therefore it must be made as difficult as possible for vendors to deny or ignore flaws in the system. Again, this requires the highest level of public scrutiny.

The ownership of source code and similar materials (such as design documentation) is another important issue where standard industry practice conflicts with the best interests of the public. Usually software vendors sell licences to use pre-compiled versions of their product and retain copyright of the code itself. However, if the source code were owned by the people instead of the vendors, we would be protected from at least two extremely undesirable scenarios: the case where a vendor or vendors go out of business; and the possibility of vendor refusing to comply with the government's wishes. First, should the vendor go out of business, the future of our electronic voting system would be significantly more secure. There being no doubt as to the ownership of the code, the Government would be considerably freer in their choice of a replacement vendor. Second, since the government would be in a position to switch to a competitor, the vendor could not make unreasonable price increases or other undesirable policy changes, nor could they refuse to make alterations/updates to the software.

The contract between Nedap/Powervote and the Irish Government explicitly retains ownership of the embedded software in the voting machines for Powervote.

> *Clause 10.1.2 Notwithstanding the vesting of ownership of the Ordered Equipment in the Customer, the Customer and Returning Officers acknowledge that the Embedded Software remains subject to a licence granted by the Suppliers and no transfer of ownership of the Embedded Software shall occur, including but without limitation any Intellectual Property Rights in the Embedded Software. The Customer and Returning Officers acknowledge that the Embedded Software is the Confidential Information of the Suppliers.*
>
> http://evoting.cs.may.ie/Documents/DoEHLGPowervoteNedapContract.doc

This is a reversal of the position laid out in the original request for tenders.

> *Clause 8.4 All software paid for and developed to Departments specification will be the property of the Department.*
>
> http://www.electronicvoting.ie/pdf/Req for tenders doc - June2000.doc

The Government has had to provide an indemnity to the Commission on Electronic Voting [CEV] in case the source code it is examining falls into the hands of competitors [Cor04]. To have allowed such a situation to develop shows a significant failure on the part of the Department to set out clear expectations that it should own any software developed for elections. The cost of the software is estimated to be €467,000 for the counting system.

It is vital that these potential conflicts of interest are recognised and addressed by those introducing electronic voting. It is not good enough for a government to rely solely on the advice, opinions and information provided by vendors. These must all be scrutinised by experts with no personal or commercial interest in the system.

3 Politics

The transparency of voting in Ireland, already eroded by the technology of the system itself, is further reduced by the way in which the introduction of the system has been managed. The procurement of evoting is being overseen by a department of the presiding government. The Minister for that department is the director of elections for one of the ruling parties for the upcoming elections. A policy of secrecy is evident, with commercial sensitivity being prioritised over public need to know. This policy is clear from the difficulty faced by those requesting information on the system, as discussed below.

Such secrecy compounds a serious problem inherent in the introduction of technology in publicly sensitive areas. Public understanding of the system is necessarily reduced as the complexity increases. This is unnecessarily exacerbated by a lack of information. Even those with the knowledge to confirm or deny the public's fears and hopes for the system cannot make comment on the suitability of the system.

There is a strong case to be made that the responsibility for decisions regarding voting technology should be taken out of government hands. While this is an issue relevant to politics, it should never become a political issue. An Electoral Commission, such as exists in the UK, would reduce the risk of mixing political motives with public interest.

3.1 Computer Science Meets Politics

Computer science is a relatively new science, only 50 years old, and the public perception of it is quite different from that of other sciences. Perhaps this is influenced by the general availability of computers and their use in practically every aspect of our daily lives. Particle accelerators are not nearly as commonplace as PCs.

No bridge would be built in the developed world without the involvement of an engineer, and yet computer systems are commonly installed by people with minimal knowledge and training. This works adequately in many low-priority situations, and so it may not be obvious that high-priority systems require greater expertise. Similarly, software is generally developed in a very ad hoc manner, which results in high failure rates. Again, this is generally a frustration rather than a major problem and is therefore acceptable in most contexts.

Computer science has, in fact, discovered laws of computation as immutable as those of physics, but the peculiar position of computer science in the public perception makes it very difficult to convey such concepts. While it may sound strange to those with no computer background, computer science tells us that we can never test a computer program enough to be absolutely certain of its behaviour.

NASA, whose employees' lives depend on the reliability of its software, are among the world's most accurate software developers, and yet they provide convincing evidence of this phenomenon. They use sophisticated techniques to reduce the faults in their software to a minimum. But studies have shown that NASA could expect 60 faults to be contained in a software project the size of the Groenendaal counting software[3] [Fis96].

[3] The IES count-software used by the Nedap/Powervote system.

The techniques mentioned above require more resources, including time, than does ad hoc development. So they are generally used only for safety critical applications such as medical equipment and driverless trains. There is a strong argument in favour of the use of these techniques in government applications such as the penalty points system used to keep track of traffic offences in the Republic of Ireland, and in electronic voting. Failures in such systems could result in innocent people going to jail, or the wrong people getting into government.

Because of public perceptions of computer science, people without adequate training may attempt tasks that require deeper knowledge. For instance, the specification of requirements for a computer system is a vital stage that requires certain expertise. It is vital that the specification for a computer system is well thought-out and covers all the requirements for the system. Mistakes made at this stage of system development can have severe effects later in the process.

The resulting lack of consultation with computer professionals has caused many problems in many walks of life, not least in the introduction of electronic voting in Ireland. Failures at the specification stage, which could have been easily identified by computer scientists, remain within the system. The most glaring example of this is the lack of a proper audit trail (see section 1.2).

3.2 Freedom of Information

Given that the people have a constitutional "right to designate the rulers of the state"[4] it is notable that ownership and scrutiny of the casting, collecting and counting of votes has become a secret matter. In response to this, concerned private citizens have made use of the Freedom of Information Acts (1997, 2003 [FoI97]) to obtain as much relevant information as possible.

Attempts to obtain technical details of the electronic voting system in Ireland have been hampered by the exemptions allowed in the Freedom of Information Acts. In particular, The Department of the Environment has relied on the trade secret and the commercial confidentiality exemptions to deny access to most of the documentation from Powervote/Nedap. Surprisingly there is no documentation from Groenendaal on the counting system. In their case the Department has refused to use a section of the Acts which provides that records held by a supplier of services are deemed to be held by the Department. This decision is under appeal to the Information Commissioner.

The Department in 2003 avoided their obligations under this section by virtue of the absence of a formal contract. There was a Letter of Intent in place under which some €30m of equipment and software were purchased. Yet the Department held that there was no current contract.

---

[4] Bunreacht Na h´Eireann/Constitution of Ireland, Article 6.

Other factors inhibiting the public in understanding this system is a marked absence of project documentation, testing schedules and testing results. No end-to-end tests[5] have been independently conducted other than the running of actual pilot elections in three constituencies in 2002. The available reports from this pilot exercise indicate that the normal reconciliation procedures completely failed. The Returning Officer proceeded on the basis of his own judgement that matters seemed to him to be in line with his expectation[6].

Mr. Joe McCarthy's personal requests under the Freedom of Information legislation have cost him €2,882 to date. Every delay allowed under the Act has been used by the Department to frustrate free access to the records. In a letter received on April 23rd, the department again refused to release certain files in the possession of the vendors of the system. Under Freedom of Information legislation, citizens may request records in the possession of "a person who is or was providing a service under a contract for services". The department refused the request on the basis that:

> *This Department does not accept that Nedap Powervote are providing a service for the Department under a contract for services.*
>
> http://www.evoting.cs.may.ie/Documents/DoEHLGDenialofContract.doc

This is in direct conflict with the contract itself (referenced earlier), which in recital 1 establishes a contract for services between Nedap/Powervote and the department.

> *WHEREAS*
> *1. The "Suppliers" will supply to the Department and Returning Officers (as hereinafter defined) designated by the Customer the Equipment (as hereinafter defined), including the Embedded Software {as hereinafter defined), Support, Project and Maintenance Services (as hereinafter defined) and as described in this Agreement.*
>
> http://evoting.cs.may.ie/Documents/DoEHLGPowervoteNedapContract.doc

3.3 History of Electronic Voting in Ireland

The introduction of electronic voting is the biggest change to the Irish electoral system since the establishment of the state over 80 years ago. The idea was introduced by the Fianna Fáil/PD government in 1999 with an Act to allow the use of actual ballot papers for research into voting methods. In 2000 a public tender was issued and it was won by the Powervote/Nedap/Groenendaal consortium.

Later in 2001 an amendment to the Electoral Act was passed allowing the Minister to approve machines for electronic voting. Remarkably, no objective or legal criteria were set for the machines or the software.

---

[5] End-to-end tests are generally considered to be a vital part of the testing process [Tam02].
[6] Paraphrased from comments made during appearances by Mr. John M. Fitzpatrick on Dublin radio station Newstalk106 and national radio station RTE1 on Friday the 16th of April.

The first enabling legislation was brought in as part of a broad, controversial bill. Debate on this bill was guillotined[7] by the Government. Several members voiced their concerns about the system at the time[8]. They were assured that the introduction of electronic voting would not go ahead without all-party consensus.

> *This Government will not proceed without unanimity and general agreement among the Members here.*
>
> - Minister Molloy, Seanad (The Irish Senate), 2001 June 14

The system was then used in three constituencies in the June 2002 General Election. The Government said the trial was successful, but others - including the authors - have grave reservations. The formal reports from the Returning Officers indicate many faults occurred [Fit02]. The results were declared without any external audit of the votes. Without further consultation, either with the Opposition or with the public, the Government decided in October 2002 to implement the system countrywide for the June 2004 local and European elections.

In 2003 a series of reports [Mcg03, Mcc03] were published questioning the integrity of the system and the process used to introduce it. A Parliamentary committee examined the matter but on December 18th 2003 the government parties applied the whip to close the debate just after the authors raised many technical questions. A publicity campaign was launched by the Government in February 2004 costing some €5m.

Public outcry continued to the extent that the Government has now appointed an ad-hoc Commission on Electronic Voting [CEV] to report on the secrecy and accuracy of the system. These terms of reference are narrow and do not allow the Commission to examine the integrity, cost or benefit of the system.

As we write, the Government is intent on pressing ahead in the face of the combined Opposition and with diminishing public support for the initiative.

4 Conclusion

Transparency is an integral part of the security of voting systems. It is vital that technology is not allowed to erode that transparency. Not only must the technology itself implement measures to ensure that it is trustworthy - which, in the current technological climate, means voter verified paper ballots - but the system must be managed in a transparent, non-partisan way.

Where democratic concerns conflict with commercial concerns - as in the case where publication of technical details may threaten intellectual property rights - the democratic concerns must be given priority. After all, businesses can move into other markets. We have only one democracy.

---

[7] This refers to a process whereby a fixed time is set for concluding debate in the Dáil. There is no further discussion at that point, the question is put to the house and voted through by Government majority against the wishes of the Opposition. It is effectively a forced change of the law by the Government.

[8] See Adrian Colley's summary of Dáil and Seanad debates on the subject of electronic voting - http://www.iol.ie/~aecolley/record.html

References

[Aus] Australian electronic voting and counting source code. http://www.elections.act.gov.au/Elecvote.html

[CEV] The webpage of the ad hoc Commission on Electronic Voting: http://www.cev.ie/

[Cha04] David Chaum. Secret-ballot receipts: True voter-verifiable elections. In *IEEE Security & Privacy (Vol. 2, No. 1)*, pages 38–47, January-February 2004.

[Cor04] Mark Brennock Chief Political Correspondent. Last-minute indemnity for e-voting commission agreed. *The Irish Times*, April 2004.

[Ele23] Electoral Act, 1923. Available online at the website of the office of the Attorney General *http://www.irishstatutebook.ie/1923_12.html*.

[Fis96] Charles Fishman. They write the right stuff. *FastCompany*, 06, Dec 1996. http://www.fastcompany.com/online/06/writestuff.html

[Fit02] John M. Fitzpatrick. Dublin county post election report, June 2002. http://evoting.cs.may.ie/Documents/PostElectJune2002.pdf

[FoI97] Freedom of Information Act, 1997. Available online at the website of the office of the Attorney General *http://www.irishstatutebook.ie/1997_13.html*.

[JRB03] Andreu Riera Jorba, Jos Antonio Ortega Ruiz, and Paul Brown. Advanced security to enable trustworthy electronic voting. In *Proceedings of the 3rd European conference on e-Government*, pages 377–384, 2003. http://www.scytl.com/docs/ECEG2003_full_paper.pdf

[Lam02] Paul Lambert. Who has their eye on your online activities? *The Sunday Business Post*, May 2002. http://archives.tcm.ie/businesspost/2002/05/05/story319171.asp

[Mcc03] Joe McCarthy. Report on the IES Counting Software. http://www.evoting.cs.may.ie/Documents/report_oniescountingsoftware.pdf

[Mcg03] Margaret McGaley, J. Paul Gibson. Electronic Voting: A Safety Critical System. http://www.evoting.cs.may.ie/Project/report.pdf

[Mer92] Rebecca T. Mercuri. Physical verifiability of computer systems. In *5th International Computer Virus and Security Conference*, March 1992.

[Mer02] Dr. Rebecca Mercuri. A better ballot box? IEEE Spectrum Online, October 2002.

[NTec] Nathean Technologies. Code review of ies build 0111 for the department of the environment, heritage and local government - page 25. http://www.electronicvoting.ie/pdf/Nathean Code Review Dec03.pdf

[Sch00] Bruce Schneier. Voting and Technology. *Crypto-Gram*, 00(12), Dec 2000. http://www.schneier.com/crypto-gram-0012.html - 1

[Soc04] Irish Computer Society. The ICS calls for audit trail in e-voting system, Mar 2004. http://www.ics.ie/article-027.shtml.

[Tam02] Louise Tamres. *Introducing Software Testing*. Addison-Wesley, 2002.

[U.S] U.S. Public Policy Committee of the Association for Computing Machinery. E-voting technology and standards. WWW page. http://www.acm.org/usacm/Issues/EVoting.htm.

[Zet03] Kim Zetter. Aussies do it right: E-voting. *Wired News*, 2003. http://www.wired.com/news/ebiz/0,1272,61045,00.html

E-Voting in Austria
Legal Requirements and First Steps

Patricia Heindl

Institute of Austrian and European Public Law
Vienna University of Economics and Business Administration
Althanstraße 39-45, 1090 Vienna, AUSTRIA
Patricia.Heindl@wu-wien.ac.at

Abstract: Whereas e-government mainly focuses on strengthening the efficiency of public government processes, it is the goal of e-democracy to improve democratic processes. Law can be defined as a communication-system between the legislative authority and the people. Using electronic media for democratic instruments can make this communication process easier. But there are also dangers and risks.
The topic e-democracy and e-voting is situated at the interface between law, politics and technology. This paper deals with the legal point of view: Which requirements does the law define for internet-based political communication, especially for computer-aided voting procedures in Austria? The law, respectively the constitutional law, defines clear and strict rules for voting and the instruments of direct democracy. If one wants to use computer-aided communication in these fields, the techniques eventually used must fulfil the relevant legal requirements.

1 Introduction

This paper deals with e-democracy and e-voting from the legal point of view. Which requirements does the law, respectively the constitutional law, define for internet-based political communication, especially for computer-aided voting procedures? The paper focusses on the legal analysis of the constitutional and statutory limits and framework. Furthermore, it concentrates on working out the preconditions, de lege lata et ferenda, for e-voting. It will also mention the first statutory amendments of implementing e-voting in Austria.

The topic e-democracy and e-voting is situated at the interface between law, politics and technology: while it is the task of legal research to define the legal preconditions and framework for electronic elections and polls, it is incumbent on technological research to develop electronic voting systems that are able to fulfil the legal guidelines. Technical knowledge is necessary to define the concrete legal issues and demands. The goal of the legal analysis is to work out the legal preconditions for the implementation of such a model.

According to this work it should be feasible to evaluate the risks and opportunities of e-voting. This might aid the Austrian legislator in deciding on the question of whether and in which fields electronic elections and voting could actually be implemented and how the constitutional and statutory principles for this task have to be drafted.

2 Democratic Instruments

Democracy means a form of political decision-making. Article 1 of the Austrian Constitution defines: "Austria is a democratic republic. Its law emanates from the people." Austria has an indirect parliamentary democracy, with some additional instruments of direct democracy. That means that law is not made by the people, but by elected representatives, the parliamentary bodies. Voting is the most important act in political decision-making by the people. Beside that the people can take part in the political decision-making process by three legal instruments of direct democracy: Referendum (Volksabstimmung), popular initiative (Volksbegehren) and public consultation (Volksbefragung).

A referendum is a national plebiscite concerning the enactment of a specific statute. With the – facultative or obligatory – referendum the people can accept or reject parliamentary resolutions at a constitutional level. The positive result of a referendum is binding. At the federal level two referenda have been undertaken so far: one concerning the question of opening a nuclear power station, the other concerning the question of joining the European Union.

The second instrument of direct democracy, the popular initiative, is a formal request by the public to introduce a matter for legislative action in the parliament. With the popular initiative a qualified number of people can raise a law-making initiative. If, at the federal level, more than 100.000 signatures are collected, the "Nationalrat" has to discuss the matter formally. But it will not be obligated to response to the request in substance. So far, there have been over 30 popular initiatives at the federal level. Nearly all of them reached the limit of 100.000 signatures; but almost none of them was followed by the parliament.

The public consultation is the weakest of the three instruments of direct democracy. With the public consultation the parliament merely collects public opinion on a special issue. Contrary to a referendum, a consultation does not have a binding effect but only an advisory character. A public consultation has not yet been undertaken at the federal level, but this instrument predominately is used at the local and regional level.

Election and the named elements of direct democracy are the constitutionally planned instruments in the process of people's decision-making. They constitute the basic democratic instruments. In a wider sense, these also include the pre-forming of political decision-making, particularly performed by political parties, organisations and pressure groups.

3 Democratic Instruments and electronic techniques

Nowadays the internet is not only used for both commercial transactions (e-commerce) and the communication between public authorities and private persons (e-government); it is also gaining ground in the central area of democracy, i.e. election and voting procedures (e-democracy)[1].

Whereas e-government mainly focuses on strengthening the efficiency of government processes, it is the goal of e-democracy to improve democratic processes. Law can be defined as a communication-system between the legislative authority and the people. Using electronic media for democratic instruments can make this communication process easier. But there are also dangers and risks.

Internet-based political communication is conceivable in all the above mentioned fields of democracy. Webpages of political and parliamentary parties or political discussion-forums in the internet are a case in point. But such type of communication is also possible with the institutionalized and constitutionally planned instruments of decision-making. The buzzwords here are "e-voting" and "e-referendum". Clearly the latter case calls for a more stringent legal framework than the former.

4 E-Voting and legal requirements

The law, respectively the constitutional law, defines clear and strict rules for voting and the instruments of direct democracy[2]. If one wants to use computer-aided communication in these fields, the techniques eventually used must fulfil the relevant legal requirements[3].

Elections to parliamentary assemblies (e.g. the federal parliament, regional state parliaments and the European Parliament), the head of state as well as to referenda are governed by constitutional law. In contrary to this elections to institutions representing public or private interests (e.g. unions of any kind) are governed by statutory law.

Considering the instrument of voting, e-voting would have to fulfil the requirements the law defines for traditional voting[4]. Austrian citizens above the age of 18 who are not excluded on account of a criminal conviction enjoy a general, immediate, equal, personal, secret and free right to vote. Austria's electoral system is based on the principle of proportional representation of contending political parties in parliament. That means that the number of votes cast for a party in principle determines the number of its seats in parliament. In general, there are no single-member districts, and no majority system, no principle of "winner takes all".

---

[1] Some authors define e-democracy as a part of e-government; see, e.g., [Sche00].
[2] Art 26, 41 Abs 2, 43, 44 Abs 3, 45, 46, 49b B-VG.
[3] For the following see also [He03], [Ma00], [Po01], [Schr01a], [Schr01b].
[4] Art 26 B-VG and NRWO *BGBl* 1992/471 idF *BGBl* I 2003/90.

Regarding the principle of general voting computer-aided communication does not seem to cause particular problems, given that e-voting is used together with traditional voting. A point yet to be proven is whether it indeed increases voter-turnout and thereby strengthens the principle of general voting. The principle of immediate voting demands that the casted votes have to reach the central voting-teller directly and non-altered. The principle of equal voting demands that each individual can cast her/his vote only once.

Parallel e-voting and traditional voting requires equality between the two voting instruments. For instance, there must be no different information on either of the two voting-"ballots" (eg: programmes of the political parties or information about the candidates). Also different error-filtering procedures might be problematic from the aspect of equality between electronic and traditional voting. Furthermore, e-voting also requires the possibility to cast unvalid votes.

But the greatest problems of e-voting lie in the principles of secret, personal and free voting. E-voting as defined in this paper is casting the votes without the supervision of an official, like voting from one's own computer at home or in the office. From this point of view e-voting poses similar problems as postal voting. In both cases the votes are not given within a secure polling booth, but the voters themselves must look for the secret and free voting act. Therefore postal voting in political elections is allowed only in some states – predominately in exceptional cases. In those states that allow postal voting – like e. g. Switzerland[5] in general or Germany[6] in exceptional cases – the constitutional barriers for e-voting seem lower than in states which have no right of distant voting.

The Austrian Constitutional Court decided, that postal voting is unconstitutional because it infringes the principles of personal and secret voting[7]. A few years later another decision by the Austrian Constitutional Court held, that Austrian nationals living abroad, must not be excluded from the right to vote only due to the lack of a permanent residence in Austria[8]. Following that a constitutional amendment was undertaken: Austrians abroad, e.g. Austrian citizens resident abroad or just staying abroad, may also vote in embassies and consulates. Even a vote in the presence of a witness will suffice. The latter case can be turned "quasi-postal" voting for Austrians abroad.

The special challenges of e-voting are twofold. On the one hand the techniques must satisfy that only legally entitled people can cast their votes and this only once. Also technical protection against electronic election fraud by hackers or technical breakdowns is necessary. On the other hand the techniques must guarantee that identification of the voter is impossible. In other words: both must be guaranteed: identity of the elector and authenticity of the casted vote and at the same time strict anonymity of the ballot paper.

---

[5] See, e.g., *Braun* in this book.
[6] See, e.g., *Volkamer* in this book.
[7] VfSlg 10.412/1985.
[8] VfSlg 12.023/1989.

Furthermore, e-voting, like traditional voting, must also allow for the possibility of ex-post examination of the election result: therefore the election-data have to stay accessible after the election day in an adequate way.

Another point is the future role of the constitutionally planned government officials in an e-voting and e-counting process.

Arguments outlined for e-voting also apply to e-referenda and e-public-consultation. E-referenda and e-voting are thus the most challenging and delicate fields of e-democracy.

The legal requirements for an "e-popular initiative" seem comparatively easier to fulfil. Here only authenticity, but no anonymity is required. From the political point of view computer-aided political communication in this element of direct democracy might have the most practical relevance. Because of electronically collecting the large numbers of signatures involved is much less time consuming and less costly than the traditional type of signature collection. This might not only lead to more frequent use of this instrument. It might also inhence opportunities to raise political initiatives for smaller and less institutionally organized groups.

5 Implementation

The implementation of e-voting for political elections of the first level (i.e. elections to the head of state, the federal parliament, regional state parliaments and the European Parliament as well as to referenda) is unconstitutional and would require a constitutional amendment. By contrast for implementing e-voting for elections to institutions representing public or private interests (e.g. unions of any kind) statutory amendments are sufficient. This is because here the voting principles are statuted not on a constitutional but on a statutory level and there is no principle of personal voting[9].

In the latter case the Austrian legislator has already taken the first steps: legal provisions for e-voting already exist for the Austrian Union of Students as well as for the Austrian Chamber of Economics[10]. Still the concreting statutory orders are missing.

Until now there have been no legally binding electronic elections in Austria. However, a first test of e-voting was undertaken parallel to the elections of the Austrian Federation of Students at the Vienna University of Economics and Business Administration[11]; another test was undertaken recently parallel to the elections of the Austrian Head of State. The implementation of e-voting in elections for unions and chambers like the named or other institutions, might help to stop the steadily declining number of people casting their votes.

---

[9] *VfSlg* 8.590/1979, 14.440/1996.
[10] § 34 Abs 4 ff *HSG*, *BGBl* I 2001/18; § 74 Abs 2 ff *WKG*, *BGBl* I 2001/153.
[11] See [Kr03], [Me01], [SK00].

Provided that all technical problems with e-voting can be solved and the legal provisions mentioned above can be fulfilled, there would still remain issues to be settled. Above all the fact of distance-voting and – in a more sociological sense – the necessarity of trusting the electronic techniques by the electors. As mentioned above: absolute protection of the secrecy voting act can not be guaranteed. If the Austrian legislator would in the future decide to implement e-voting in political elections, this possibility should always be restricted to those groups who are not able to cast their votes within the official polling booth.

References

[He03] Heindl, P., e-voting und e-democracy aus verfassungsrechtlicher Sicht, in: E. Schweighofer et al (Hrsg.), Zwischen Rechtstheorie und e-Government, Wien 2003, 279 ff.

[Kr03] Krimmer, R., E-Voting in Österreich, in: E. Schweighofer et al (Hrsg.), Zwischen Rechtstheorie und e-Government, Wien 2003, 271 ff.

[Ma00] Marschitz, W., Internetvoting, in: Österreichische Monatshefte (2000), http://www.plattform.or.at/download/POP_Art_Internetvoting.pdf (15. 1. 2004).

[Me01] Menzel, T., E-Voting an österreichische Hochschulen, in: E. Schweighofer et al (Hrsg.), Auf dem Weg zur ePerson, Wien 2001, 281 ff.

[Po01] Poier, K., Grundrechte und E-Voting, in: Österreichische Juristenkommission (Hrsg.), Grundrechte in der Informationsgesellschaft, Wien 2001, 102 ff.

[Sche00] Schefbeck, G., Elektronische Demokratie, in: E. Schweighofer, T. Menzel (Hrsg.), E-Commerce und E-Government, Wien 2000, 89 ff.

[Sche01] Schefbeck, G., Aktuelle Trends in der E-Demokratie, in: E.Schweighofer et al (Hrsg.), Aufdem Weg zur ePerson, Wien 2001, 293 ff.

[SK00] Schinagl, W., Kilches R., Online Wahlen und E-Voting – Entwicklungstendenzen zu elektronischen Wirtschaftskammer-Wahlen im Jahr 2005, in: D. Pauger (GesRd.), Neue Medien – 3. Fakultätstag der Rechtswissenschaftlichen Fakultät 12. Mai 2000 (oJ.), 291 ff.

[Schr01a] Schreiner, H., Art 26 B-VG, in: H. P. Rill und H. Schäffer (Hrsg.), Bundesverfassungsrecht – Kommentar, Wien 2001, Rz 57.

[Schr01b] Schreiner, H., Wahlen per Mausklick – rechtliche Überlegungen zum I-Voting, in: E.Schweighofer et al (Hrsg.), Auf dem Weg zur ePerson, Wien 2001, 258 ff.

Security Assets in E-Voting

Alexander Prosser, Robert Kofler, Robert Krimmer, Martin Karl Unger

Institute for Information Processing, Information Business and Process Management
Department Production Management
Vienna University of Economics and Business Administration
A-1200 Vienna, AUSTRIA
[Alexander.Prosser | Robert.Kofler | Robert.Krimmer | Martin.Unger}@wu-wien.ac.at

Abstract: As discussed in the literature [PrMü01; Rub04; Phi02] e-voting faces a lot of threats. The purpose of this paper is to give a systematically ordered overview of attacks against e-voting and to show one solution to the issues. The challenge is to provide identification and anonymity at the same time and to exclude the possibility of fraudulent manipulations by the server administration, the voter, and any third party.

1 Protocol Issues

1.1 Two-Stage Versus One-Stage Voting Protocols

In a fundamental contribution, Nurmi et al. [NSS91] identified two building blocks in an electronic voting system: (i) Voter identification and registration for e-voting and (ii) vote casting. These steps can be provided in one Internet session (one-step protocol); but here the identification may be used to trace the identity of the vote via the IP address or temporary files. This issue is avoided by a two-stage procedure, which strictly separates voter identification and vote-casting. But the advantage comes at a price, as the result of successful identification (voting token) has to be stored at the voter to be used later to cast a vote. Figures 1a and 1b provide an overview of the two stages.

Registration phase:

The voter applies for a voting token. The system performs a check of his credentials and a check for multiple application. If this is his first attempt, the voter will receive a voting token which he can use anonymously to cast a vote later. If not, the system performs a restart procedure, which always issues the same token to the applicant, which is stored in the database of the regis-tration service.

At the end of the process, the voter checks the authenticity and integrity of the token and stores it either on a smart card or on another media, e.g. a USB token.

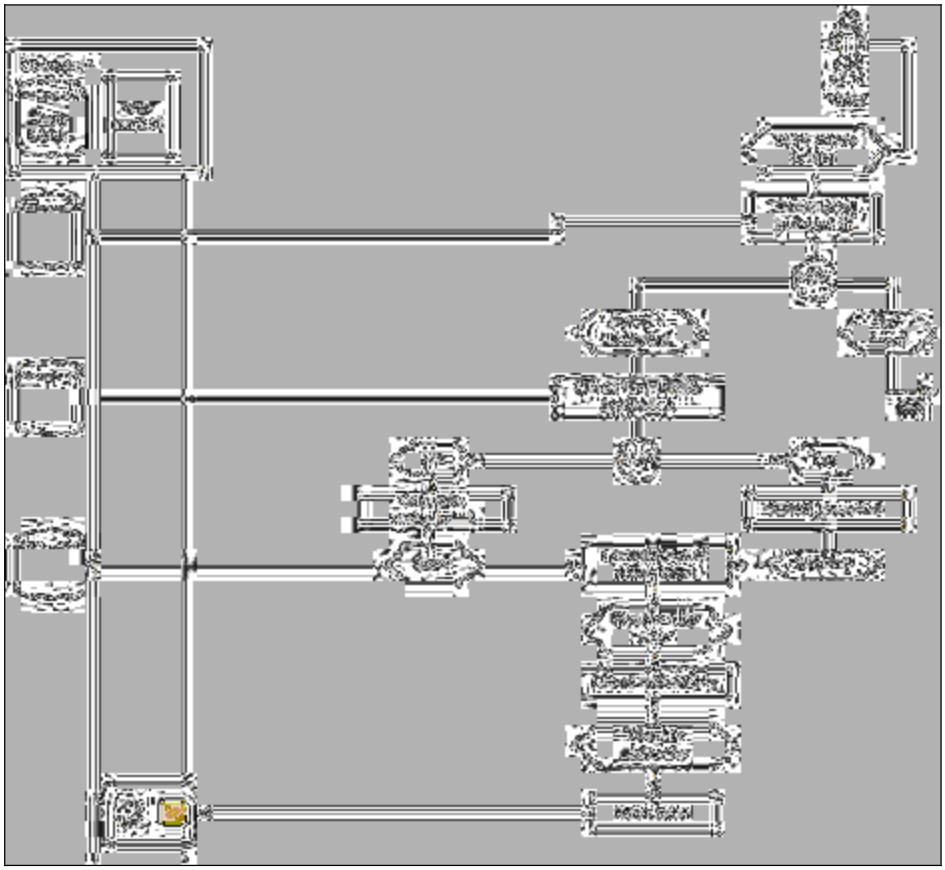


Figure 1a: Registration phase

Voting phase:

The voting application reads the voting token from the storage device and sends it to the ballot box system, which verifies its authenticity and checks for duplicates. If the checks are successful, the voter will receive a ballot sheet, which must be protected against manipulation. The voter fills in the ballot sheet and casts a vote. There is a precaution mechanism that challenges the voter before the vote is actually cast to prevent precipitate or "junk" votes.

Finally the voter receives a confirmation that the vote has been cast successfully.

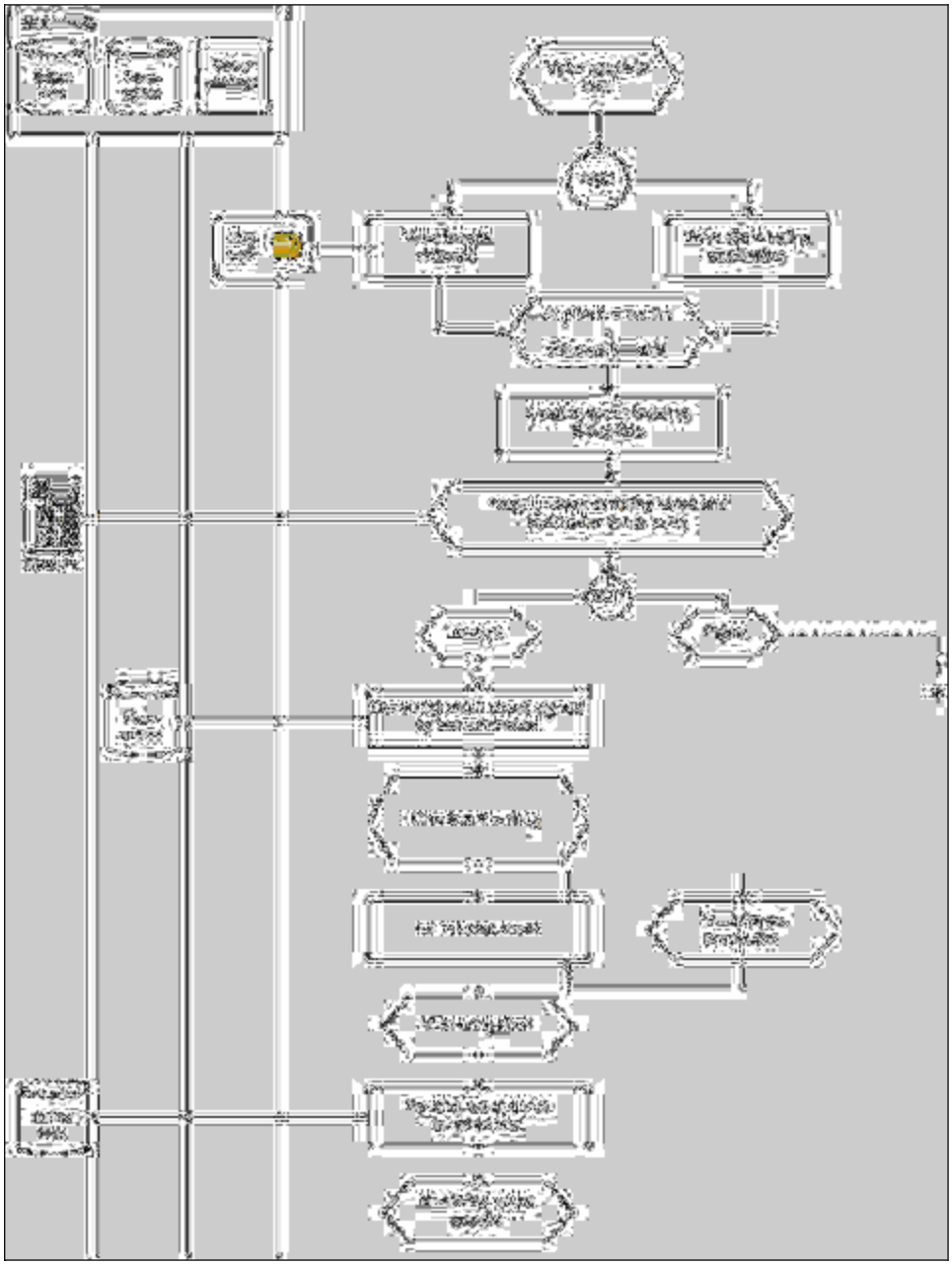


Figure 1b: Voting phase

Eventually, there may also be also a facility for the voter to check whether his vote was counted correctly and entered the tally.

1.2 Threat Scenarios

1.2.1 Threats during Registration

Beginning with the initiation of the process there must be a possibility to verify the authenticity of the voter's application and/or visited webpage [FFW99]. The next step is the application for the selected election (there can be more than one election at the same time). When the user transmits his personal ID or related information, it must be protected from modification, re-send attacks, content sniffing (the fact whether somebody is going to vote should remain private) and all forms of faked identities. The voter's identification and assignment to a constituency must be established beyond doubt and must be protected from manipulation by the voter as well as by the system administration.

Also the constituency the voter belongs to should be protected from manipulation (eg., a voter "re-registers" himself to another constituency, where he perceives that the vote would probably have a higher marginal value). This is particularly an issue in two-stage voting protocols, as the token issued on registration must be used anonymously and hence, has to include the constituency information, so that the vote can be assigned correctly, even though the voter will not be identified at the voting stage.

On the voting server side, it must be assured that multiple (malicious) applications from one person can be handled. The Server administrator must not be able to change a voter's constituency without detection; also selective denial of service to registrants by the administration must be prevented. In addition, the administration must not be able to create fake voting tokens or to-kens on behalf of people, who did not register.

Furthermore the administrator must not delete records from the registration database unrecognized. An audit trail must be producible that links every voting token issued to an eligible voter, showing that every voter also had the opportunity to obtain a voting token but once.

When the voting token is received by the client, some integrity checks should be done before the token is stored on a secure media or if no secure media is available we need equivalent methods to prevent others from using it (eg, a third person, Trojan, virus or other malign application).

1.2.2 Threats during the Voting Phase

Authenticity, validity and integrity of a voting token must be assured, at the same time, the token must be usably in a completely anonymous way. The voter uses the token to apply for a ballot sheet. It has to be assured that the ballot sheet is not modified during transmission by a man in the middle or by the administrator of the ballot box - therefore the voter needs some guarantee that this is the correct ballot sheet he applied for. Duplicate use of voting tokens has to be prevented.

Also, it has to be assured that ballot sheets cannot be manipulated by the server administration and are delivered to the voter authentically. When the voting software renders and displays the ballot sheet, it should use a secure viewer so that no virus or Trojan horse application can neither change the ballot sheet, nor forward the voter's choice to a third party. As the content of the vote should be kept secret even from the election system administration until the ballot box is opened, the vote should also be encrypted in a way that the administration cannot read or manipulate the vote.

The ballot box server environment must prevent the administration from denying access, deleting, inserting or modifying ballot sheets and it must prevent multiple usages of voting tokens. In a two-stage protocol the administrator must not be able to separate the voting token from the ballot sheet. And most importantly, voter anonymity must be guaranteed vis-à-vis the election administration as well as any third party.

The last step in the voting process is a return receipt which shows the voter that his ballot sheet was received. However, no proof must be possible, how a voter voted, as this would enable vote buying and pressured votes. On request, an audit trail must be produced linking the token used and the fact that a ballot sheet was obtained and stored. This audit trail must not corrupt anonymity, but it has to be manipulation-proof, also by the election administration. This also serves as a defence against unfounded objections and complaints from voters, candidates or third parties maintaining irregularities in the voting process in order to sabotage or discredit the election.

1.2.3 Levels of Security

In the discussion of e-voting security, one has to distinguish between organizational and technical security. Precautions are organizational, if they rely on the behaviour of agents and their compliance to rules. Examples would be

- Information stored on two server systems, which, once joined, would corrupt anonymity; the server administrators are obliged (possibly under oath) not to communicate data.
- Servers locked into a safe room to prevent tampering.
- A witness, who (digitally or on paper) signs that a certain document was filled in at a certain time and in a certain place.

Technical precautions provide a technical guarantee against defined manipulations or threats; it does not rely on any agent's compliance with proper procedures. Examples would be

- Cryptographic encoding of ballot sheets to prevent their manipulation by the server administration.
- A blind signature [Chau82] or ANDOS [BCR87] procedure to prevent the tracing of voting tokens.

It should be noted that technical security cannot be absolute – at some stage organizational security has to come in. Digital signature cards, for example, provide an extremely high level of technical security; however, when the card is issued,

organizational precautions against manipulations are necessary to prevent, for example, the card PIN entered by the card holder from being recorded and later to be used in conjunction with the stolen signature card. Hence, the decisive question is, at which level technical security ends and where reliance on organizational measures starts. The following section provides a model to asses this issue in the field of e-voting.

2 Six Aspects of E-Voting Security

Six aspects can be identified in e-voting security to be fulfilled either by organizational or technical/algorithmic arrangements. The degree to which an e-voting system relies on technical security constitutes the essential quality parameter of such a system [IPI01].

The aspects are: (i) Permanent voter anonymity, (ii) voter identification and ascertainment of eligibility, (iii) resistance against all forms of manipulation (third party, voter or administration staff), (iv) prevention of vote buying, (v) a complete audit trail for authorities and voters, (vi) prevention of sabotage and attempts to discredit the election. Figure 2 summarizes these dimensions defining a 4 point scale for each dimension (from within: (1) slight to no protection, (2) corruptible with medium determination, (3) high degree of protection, (4) virtually unbreakable). For each dimension, the model defines how far technical safeguards apply (the line joining the dimensions). Beyond this level, organizational safeguards may apply. However, it remains to be ascertained from case to case, whether organizational protection is viable.

Some of the above goals are in clear antinomy. An e-voting system, for example, designed to perfectly meet requirements (ii) to (vi) cannot technically guarantee voter anonymity (see Figure 2). In this case, organizational safeguards would have to be provided.

On the other hand a system, designed to meet the requirement of anonymity only (“naive anonymity”) would neglect the other goals and would have to provide purely organizational safe-guards (Figure 3).

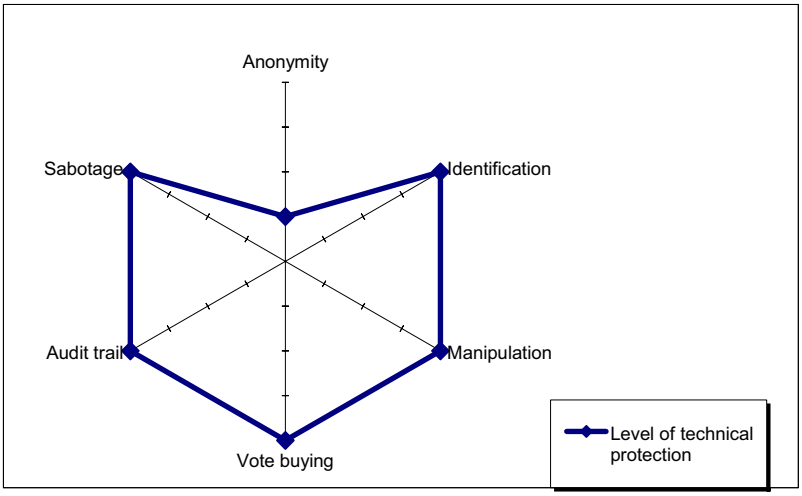


Figure 2: Fully auditable system, resistant against sabotage and manipulation

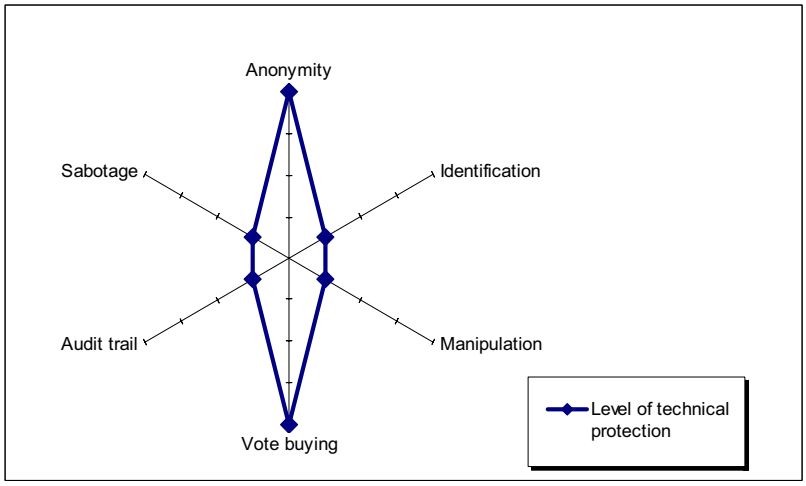


Figure 3: "Naively" anonymous system

The question arises, whether a voting protocol can be defined that combines technical safe-guards for voter anonymity as well as identification and reproducibility.

3 The Protocol of e-voting.at

The participating parties are (i) the voter, (ii) the registration authority maintaining the voter register, (iii) the electronic ballot box, (iv) a third party, such as a trust centre or the Privacy Protection Committee.

Registration:

1. The registrator has one signature key pair (e, d) per constituency c; each trust centre participating in the election has its (ε, δ).
2. The voter sends his voter ID to the registrator, which after checking the voter's eligibility answers with *c* and the appropriate e. The voter also polls the trust centre for ε.
3. The voter creates random tokens t and τ preparing them for a blind RSA signature ($b(t), b(\tau)$). c, $b(t)$ and a standard text applying for a signed e-voting token is sent to the registrator, which after checking the credentials again blindly signs and returns $d(b(t))$. The voter removes the blinding layer and obtains $d(t)$.
4. The voter obtains $\delta(\tau)$ in a similar way from the trust centre.

Storage:

The voter stores $t, d(t), \tau, \delta(\tau), c$ on a secure media (for the role of smart cards in e-voting, cf. [PKKU04]).

Voting:

1. Prior to the election, the members of the election committee form RSA key pairs (k, k') and make their respective encryption keys k' known to the ballot box server.
2. On election day, the voter sends $t, d(t), \tau, \delta(\tau), c$ to the ballot box server, which knows all relevant e and ε.
3. If the ballot box can authenticate the tokens for the constituency indicated and if they have not already been used, it returns an empty ballot sheet BS and the relevant k'.
4. The voter codes the filled-in BS with k' and untamperably links the tokens to this $k'(BS)$. The ballot box once again checks the tokens and stores the ballot.
5. The ballot box issues a receipt, which does not contain any information on the vote cast.

After the election finished, the members of the election committee reveal their secret decryption key k and the ballot sheets are decrypted. The above protocol as currently implemented does not enable majority decisions by the election committee, or enables the replacement of an election committee member who had an accident, lost his key, wants to sabotage the election etc. A solution for quorum-based decisions is provided in [PKKU04a].

4 Threats and Security

Let us analyze the security aspects identified in Figures 2 and 3:

Anonymity
Since the token is issued with a blind signature it cannot be traced back to the user. On election day, the voter uses the token as means of authentication only. The only means of intercepting the token and to corrupt anonymity is the voter's PC. This can be ruled out, if the decisive parts of the voting protocol (such as the resolution of the blind signature provided by the registration server) are performed in the secure environment of a smart card (eg., a signature card).

Identification
Authenticity can be provided by signing the application for a voting token using a digital signature card. If this is also a citizen card (in Austria cf. [HoKa04]), the voter can also be identified. Authenticity on election day is only provided by the voting token. If this token is not stored in the secure environment of a PIN protected area on a smart card, the token has to be password-protected.

Manipulation
Manipulation by a third party can happen in transmission or on the voter's PC. The former is prevented by standard encryption, such as SSL/TLS (IETF RFC 2246), the latter by again performing the decisive protocol elements in a secure and tamper-proof environment.

Manipulation by the administration can affect:
(i) The issue of fake tokens, which is prevented by the second authority, whose token is needed to cast a vote as well.

(ii) The manipulation of votes, which is prevented by encryption of the ballot sheet with the keys of the members of the election committee.

(iii) The insertion of votes, which is prevented by the same mechanism as (i) and by the fact that the token is re-submitted and inextricably linked to the filled-in ballot sheet when it is submitted.

(iv) The deletion of votes can be prevented when the tokens are published for which a vote was cast and voters are provided with a signed conformation by the ballot box server that a vote has been cast for this token.

Vote Buying
The voter is given a receipt without any reference to the actual vote cast. This would also be impossible, as the vote submitted to the ballot box server is coded with the election committee keys.

Audit Trail
The audit trail is two-fold corresponding to the two-stage protocol: (i) it is reproducible, which member of the electorate sent in a signed application to vote electronically and

whether she received a token; (ii) which token was sent in to obtain a ballot sheet and which vote was cast for the respective token. Of course, the link between (i) and (ii) is not reproducible; this is the essence of a two-stage protocol. (iii) Each signed application must contain a corresponding one from a second authority.

Sabotage

Since there is a complete audit trail, assertions of irregularities can be dealt with satisfactorily.

The protocol described in this paper has been implemented and used in two test elections parallel to the Student Union election in 2003 [PKK03] and the Austrian Federal Presidential election in 2004 [PKKU04b].

References

[BCR87] Brassard, G., Crepeau, C., Robert, J.-M.: All-or-Nothing Disclosure of Secrets. In: Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86, Berlin, Springer-Verlag, 1987, pp. 234-238

[Chau82] Chaum, D.: Blind Signatures for Untraceable Payments in: Chaum, D., Rivest, R.L., Sherman A.T. (eds): Advances in Cryptology, Proceedings of Crypto 82, pp. 199-203

[HoKa04] Hollosi, A., Karlinger, G.: Einführung in die österreichische Bürgerkarte; Bundeskanzleramt, Stabsstelle IKT-Strategie des Bundes, Technik und Standards, Vienna, 2004, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html (10.6.2004)

[IPI01] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC), 2001 http://www.internetpolicy.org/research/e_voting_report.pdf (2001-11-20)

[FFW99] Feghhi, J., Feghhi, J., Williams, P.: Digital Certificates – Applied Internet Security; Addison-Wesley, Reading, 1999

[NSS91] Nurmi, H., Salomaa, A., Santean, L.: Secret ballot elections in computer networks; Computers and Security 36 (10), 1991, pp. 553-560

[Phi02] Philippsen M.: Internetwahlen – Demokratische Wahlen über das Internet; Informatik Spektrum 25(2) 2002, pp. 138-150

[PKK03] Prosser, A., Kofler, R., Krimmer, R.: Deploying Electronic Democracy for Public Corporations. In: Traunmüller, R. (ed.): Electronic Government, LNCS 2739(2003), pp. 234-239

[PKKU04] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: The Role of Digital Signature Cards in Electronic Voting. Proceedings of 37th Annual Hawaii International Conference on System Sciences (CD/ROM), Computer Society Press, 2004

[PKKU04a] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: Implementation of Quorum-based Decisions in an Election Committee; to appear in Traunmüller, R. (ed.) E-Government; Lecture Notes in Computer Science, Springer, 2004

[PKKU04b] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: e-Voting Wahltest zur Bundespräsidentschaftswahl 2004, Arbeitsbericht zum Tätigkeitsfeld Wirtschaftsinformatik, Informationsverarbeitung und Informationswirtschaft 01/2004, Wirtschaftsuniversität Wien, 2004

[PrMü01] Prosser, A., Müller-Török, R.: Electronic Voting via the Internet; Int. Conf. on Enterprise Information Systems ICEIS 2001, Setùbal, pp. 1061-1066

[Rub04] Rubin, A.: Security Considerations for Remote Electronic Voting over the Internet http://avirubin.com/e-voting.security.pdf (23.5.2004)

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER - Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods - Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahnič (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 - Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement - Erfahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometric and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society

The titles can be purchased at:
Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14
53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de

GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of "Seminars", "Proceedings", "Monographs" and "Dissertation Award", current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: http://www.gi-ev.de/service/publikationen/lni/

Robert Krimmer (Ed.): Electronic Voting 2006

GI-Edition

Lecture Notes in Informatics

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2nd to 4th of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.

P-86

Proceedings

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe,
ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

Gesellschaft für Informatik 2006

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-86

ISBN 978-3-88579-180-3
ISSN 1617-5468

Volume Editor
Mag. Robert Krimmer
E-Voting.CC
Competence Center for Electronic Participation and Electronic Voting
Liechtensteinstrasse 143/3
A-1090 Vienna, Austria
Email: r.krimmer@e-voting.cc

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

It is now two years since we last met at Castle Hofen to discuss important topics involved with electronic voting. Back then it was intended to bring together interested people in e-voting. What was first planned as a sole academic meeting in the field of information technology has fast become a get-to-gether of academia, administration and vendors in the field. This is for sure due to the high level of interdisciplinary and high interest on all sides.

Two years ago we listened to the presentation of the Council of Europe recommendation on legal, technical and organisational on electronic voting or many other ambitious plans on implementing electronic voting.

Looking at this year's contributions we can easily see the fast development the field has undertaken. First of all thanks to the support of the Council of Europe our meeting serves as an academic review meeting for the back then discussed recommendation. Second we also have first empirical data on the actual use of e-voting in legally binding political elections and deal with so important topics like the observation of electronic voting. It is also good to see that the discussion on electronic voting is becoming a global one. While in 2004 the attendees of the workshop came from 11 countries, this year we have participants coming from nearly 30 different countries as far away like New Zealand or Brazil.

For our call of papers we received over 40 submissions of which we had to select the 20 best for presentation. This was done in a double-blind review process which wouldn't have been possible without the tremendous effort the programme committee members and the additional reviewers put in the process.

Special thanks go to the Council of Europe for their support in organizing this conference. I wish to thank Simon French, Wolfgang Polasek, David Rios, and Simon French as well as the remaining members of the TED steering committee for supporting once more our workshop.

Further thanks go to the German Society of Informatics and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Computer Society, the Federal Computing Centre for their continued support.

Without the help of the programme committee, especially Nadja Braun and Thomas Buchsbaum, who were always available with their advice that helped shaping the workshop the way it is today.

Finally I would like to thank Terry Davis general secretary of the Council of Europe and Jürgen Weiss vice chairman of the Austrian Federal Council that the conference can take place under their auspices.

Vienna, August 2006 Robert Krimmer

Programme Committee

- Frank Bannister, Ireland
- Nadja Braun, Switzerland
- Thomas Buchsbaum, Austria
- Tony Cresswell, USA
- Rüdiger Grimm, Germany
- Marjin Janssen, The Netherlands
- Simon French, United Kingdom
- Robert Krimmer, Austria (Chairman)
- Hannu Nurmi, Finland
- Wolfgang Polasek, Switzerland
- Alexander Prosser, Austria
- David Rios, Spain
- Fabrizio Ruggeri, Italy
- Daniel Tokaji, USA
- Melanie Volkamer, Germany
- Maria Wimmer, Germany

Additional Reviewers

- Bernard van Acker, Belgium
- Daniel Brändli, Switzerland
- Craig Burton, Australia
- Fiorella De Cindio, Italy
- Astrid Dickinger, Austria
- Sonja Hof, Switzerland
- Jason Kitkat, United Kingdom
- Nico Lange, Finland
- Herbert Leitold, Austria
- Margaret McGaley, Ireland
- Anne-Marie Oostveen, Netherlands
- Jordi Puiggali, Spain
- Peter Reichstädter, Austria
- Michael Remmert, France
- Thomas Roessler, Austria
- Ronald Vogt, Germany
- Peter Wolf, Bosnia and Herzegovina

Organizing Committee

- Friederike Findler, Austria
- Sandra Huber, Austria
- Ilse Klanner, Austria
- Katharina Kozlik, Austria (Chairman)
- Wolf-Heinrich Reuter, Austria
- Stefan Triessnig, Austria

Sponsors

Co-Organizers

Webcast

All presentations are available in Audio & Video including slides at
http://www.e-voting.cc/2006 with the help of

Content

Overview

Robert Krimmer

E-Voting.CC
Competence Center for Electronic Participation and Electronic Voting
Liechtensteinstrasse 143/3
A-1090 Vienna, Austria
r.krimmer@e-voting.cc

Although the recent developments might give the impression that e-voting is an invention of the last decades, in fact it was one of the first applications of computers in public environments. First voting machines even date back to the end of the 19th century. The idea of modernising elections through electronic means has been an issue of visionary people early on. Forward thinkers like Fromm, Fuller, Arterton or Rheingold [From55, Full63, Arte87, Rhei93] have come up with ideas on how electronic voting could change and enhance democracy as such.

In the past years many governments have started to adopt computer-supported applications for their administrative processes; applications range from the simple download of forms to Internet-based submission of applications. Amongst these the most controversial application is electronic voting, which stands for the use of electronic means in elections. Motives for implementing electronic voting procedures are manifold, amongst the most important are as noted in the 2004 Council of Europe recommendation for electronic voting [CoE04, Remm04]:

1. enabling mobility of the voters
2. facilitating the participation in elections from abroad
3. raising voter turnout by offering additional channels
4. widening access for citizens with disabilities
5. reducing cost
6. delivering voting results reliably and more quickly

While the first four are benefits for citizens in the field comfort and participation and last two are benefits for administrators in the field of process workflows and costs. Also the last two are benefits that hold for any form of e-voting while the first four are mainly to be found for remote electronic voting. This might explain part of the controversies with citizens involved with electronic voting machines. In transition democracies the last two reasons are especially important as they promise to solve on one hand problems with alphabetisation of the population and problems with infrastructure in regard to delivering the results in time.

Therefore electronic voting not only serves as aid in counting the votes, by now they support all three main voting processes:

1. Pre-Election Phase: Identification of the voter, checking of eligibility
2. Election Phase: Casting the vote
3. Post-Election Phase: Counting of the votes.

Besides the discussion of polling place e-voting the debate in many countries specially concentrates on remote electronic voting, i.e. through the Internet and shares the common problems of remote voting procedures like vote coercion and buying.

<table>
<tr><th>Environment
Medium</th><th>Controlled</th><th>Uncontrolled</th><th></th></tr>
<tr><td>Paper</td><td>Polling Place</td><td>Postal Voting</td><td rowspan="3">Counting Machines</td></tr>
<tr><td rowspan="2">Electronic</td><td>Stand-Alone
Electronic Voting Machine</td><td rowspan="2">Remote
Electronic Voting
(PC, Cell Phone)</td></tr>
<tr><td>Networked Electronic
Voting Machine</td></tr>
<tr><td></td><td colspan="2">Networked Kiosk Electronic Voting</td><td></td></tr>
</table>

Figure 1: Forms of Voting [cp. VoKr06]

In general electronic voting is based on the separation of voter identification and vote casting as identified by Nurmi [NSS91]. Basic technologies for identifying voters are [VoKr06]:

- Username and passwords [knowledge]
- Transaction Numbers (TAN) [possession]
- Smart Cards [possession and knowledge]
- Biometric properties [might also be combined with the above].

For anonymity purposes these are [VoKr06]:

- Organisational pre-registration [handing out TANs]
- Hidden result calculation [using hardware security modules]
- Blind signatures

While the worldwide implementation approaches might be different in detail, many efforts still share the criticism by the public in regard to the lack of transparency of the application itself. Oostveen and van den Besselaar have shown that trust in the e-voting process is not dependent on the actual level of security but on the user's belief how secure the system is. This belief is largely dependent on the transparency of a system and here the 'main challenge for electronic voting [comes in:] the lack of transparency' [OoBe05].

The programme committee therefore tried to select the best papers based on their relevance to the conference topics and their quality to contribute to the growing need in qualified and argued discussion of the emerging topic of e-voting. The papers are grouped in nine sessions, which address the topics of experiences made with e-voting, social, technical, political issues as well as legal and democratic issues of e-voting, analyzing solutions for the uncontrolled environment, redesigning workflows for e-voting, observation, implementation and security of e-voting and finally political views and democratic challenges.

In session one the first hands-on experiences with legally binding political elections are presented. It includes two papers with reports from Estonia and Switzerland. *Ülle Madise* and *Tarvi Martens* explain the technological and legal point of view in Estonia as well as empirical findings on who were the voters in the worldwide first country-wide binding internet e-voting. *Nadja Braun* and *Daniel Brändli* then evaluate the swiss e-voting pilot projects and depict a road ahead for the time after the first trials.

The second session then tries to give an interdisciplinary view on the topic by looking at deep technological advances, political issues and social implications. It starts with a paper by *Ana Gómez*, *Sergio Sánchez Garcia*, and *Emilia Pérez Belleboni* who present an advanced technological solution based on a java card for future enhancement of smart cards to best suit electronic voting. In the second paper *Jordi Barrat Esteve* tries to answer the questions do we really need electronic voting and in which way (not) to take to implement it. *Laurence Monnoyer-Smith* then brings up the topic of the change of the voting ritual. This discussion is very necessary as the experiences in Ireland have shown us.

Session three addresses the legal and democratic issues of e-voting. *Rosa M. Fernández*, *Esther González*, and *José Manuel Vera* present the legal regulations set for e-voting in the autonomous Spanish Basque community. The experiences with e-voting in Brazil are presented by *José Rodrigues-Filho*, *Cynthia J. Alexander*, and *Luciano C. Batista*. They give a report about how e-voting have unwished results when implemented in the wrong way.

In the forth session we analyze how possible influence on the voter can be handled in the uncontrolled environment. *Melanie Volkamer* and *Rüdiger Grimm* first discuss the possibility of multiple casting a vote. *Gerhard Skagestein*, *Are Vegard Haug*, *Einar Nødtvedt*, and *Judith Rossebø* then conclude with an architecture for trust building measures in the uncontrolled environment.

The topic of the fifth session is the election process and to support and redesign it. *Alexandros Xenakis* and *Ann Macintosh* present an methodology on how to re-engineer an electoral process to make it fit for e-voting. *Goran Obradovic*, *James Hoover*, *Nick Ikonomakis* and *John Poulos* then present their solution for a fully supported electronically supported election workflow.

Session six's topic is observing and testing of electronic voting. *João Falcão e Cunha*, *Mário Jorge Leitão*, *João Pascoal Faria*, *Miguel Pimenta Monteiro*, and *Maria Antónia Carravilla* present their methodology used to test e-voting systems used for Portuguese parliamentary elections. The election specialist *Kåre Vollan* presents the problems of to observing electronic voting. *Jörn Schweisgut* then concludes with a technical solution to allow for observers in e-voting and solve the problem of voter coercion.

The implementation of e-voting is discussed in session seven. *Carol Boughton* presents the eVACS system and how it maintains the democratic values. Letizia Caporusso, *Carlo Buzzi*, *Giolo Fele*, *Pierangelo Peri*, and *Francesca Sartori* presents results of an implementation process of an Italian e-voting project and propose a careful approach.

The session on security for e-voting is the eighth. In an collaboration effort *Rüdiger Grimm*, *Robert Krimmer*, *Nils Meissner*, *Kai Reinhard*, *Melanie Volkamer* and *Marcel Weinand* present the approach of the Gesellschaft für Informatik on how to develop a protection profile. *Klaus Diehl* and *Sonja Weddeling* then present how their system is guaranteeing the German election principles.

The last session then gives room to democratic challenges and the politician's view on e-voting. *Joan Josep Piles*, *José Ruiz*, and *José Maria Moreno-Jiménez* present the challenges their e-voting proposal for what they call the e-cognocracy. Finally *Tina Jukić* and *Mirko Vintar* bring the often forgotten politicians on the table and present their view that might give answers to some questions we raised before.

As you can see this proceedings volume gives a heterogeneous picture of what is state of the art and what are current topics of discussion in the e-voting community. This gives good hope for a successful continuation of our e-voting workshop at Castle Hofen in Austria. For the future it will also be interesting to develop a road map of future research which would then guide the development and implementation of e-voting worldwide.

References

[Arte87] Arterton, C.: Teledemocracy: can technology protect democracy? Sage Publications, Newbury Park, Washington D.C, 1987.

[CoE04] Council of Europe (2004): Electronic Governance. Recommendation Rec(2004)15 and explanatory memorandum, Council of Europe, Strassbourg, 42 pages.

[From55] Fromm, E: The Sance Society. New York, Rinehart, 1955.

[Full63] Fuller, B. R.: No more Secondhand God, Southern Illinois University Press, 1963.

[OoBe05] Oostveen, A., van den Besselaar, P.: Trust, Identity, and the Effects of Voting Technologies on Voting Behavior, Social Science Computer Review (23) 3, 2005, pp. 304-311

[Remm04] Remmert, M.: Towards European Standards on Electronic Voting. In: Prosser, A., Krimmer, R.: Proceedings of the 1st ESF TED Workshop on Electronic Voting, GI LNI P-47, Bregenz, 2004, pp. 13-16.

[Rhei93] Rheingold, H.: The Virtual Community, Addison-Wesley, Reading, 312 pages, 1993.

[VoKr06] Volkamer, M., Krimmer, R.: Die Online-Wahl auf dem Weg zum Durchbruch. Informatik Spektrum, Springer,

Session 1: E-Voting Experiences

E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world

Ülle Madise[1,2], **Tarvi Martens**[1]

[1] National Electoral Committee
[2] Tallinn University of Technology
Lossi plats 1 a
15165 Tallinn Estonia
ylle.madise@riigikontroll.ee
tarvi@sk.ee

Abstract: At Estonian local elections in October 2005 for the first time in the world binding country-wide remote Internet voting took place: whole Estonian electorate had a possibility to cast the vote via Internet. Approximately 2 % of actual voters made use of this possibility. The e-voting surveys show that the attitude of the Estonian public toward e-voting was and is positive; gender, income, education, type of settlement and even age are no important factors by choosing e-voting from all voting channels; the use of e-voting possibility depends mostly on the trust in the procedure of e-voting and E-voting in itself does not produce any political effects. Estonian e-voting experience in 2005 reassures the hypothesis that e-voting does not raise the voting activity of people who never take part in elections, but it can encourage the participation of voters who vote sometimes. Thus, e-voting could slow down the trend of falling participation. Despite successful e-voting experience in October 2005, the political debate around e-voting has started in Riigikogu (Estonian Parliament) again. If the e-voting provisions will not be excluded from the law, the next country-wide e-voting in Estonia is taking place February-March 2007 by next Riigikogu elections.

1 Background

Estonia is widely credited to be a pioneer in e-governance and e-democracy. The use of digital channels for different services is steadily widening, nearly half of households have a computer at home and more than 4/5 of those are connected to the Internet. There are 55 public Internet access points per 100 000 inhabitants and all schools are connected to the Internet. Estonia is the only country in the world, where ID card with remote identification and binding digital signature functions is compulsory whereby ~70 % of Estonian inhabitants are already cardholders.[1] Therefore introducing e-voting[2] was a logical step to take and e-voting could be seen as an essential convenience in an information society, like using Internet for sending tax declaration etc.

The declared aim of the launching of online voting was to increase voter turnout and fight against political alienation. The participation rate at local government council elections in Estonia is usually ~ 50 % and at parliamentary elections ~ 10 % higher. The voter turnout did not exceed 70 % even at the constitutional referendum in 1992. So, the problem of low turnout really exists in Estonia. Since especially young voters' turnout is expected to rise, the most active supporters of e-voting are those parties, who hope to gain additional votes from an increased turnout. The angriest opponents seem to be those parties, who would probably lose their position in respective representative bodies that are composed on the principle of proportionality.

2 Theoretical fears and threats

The political agreement to introduce e-voting in Estonia beginning at 2005 elections was made in 2002[3]. In the discussion about introduction of e-voting classical arguments about conformity of the e-voting with the principles of fair elections incl reliability of electronic voting systems were changed, whereby one of typical arguments against e-voting was that people who have no commitment to go to the polling station to execute their citizen's duty, should not participate in governing at all, which attitude contradicts to the axiom that the higher the turnout is the better. The threats and fears around e-voting can be divided into two major groups:

- Purely political fears: some parties are afraid that the possibility to e-vote brings some people to vote, who otherwise would not participate. If those, who otherwise would not participate, would vote, the position of those parties, whose supporters prefer traditional voting in the polling station (or if said directly: who are ready to go to the polling station), could worsen. This fear is based on the assumption that possible e-votes are not divided proportionally between the parties;

---

[1] See the ID-card webpage in English: http://www.id.ee/pages.php/030301 [accessed on 01-05-2006].
[2] The public in Estonia is used to the meaning of e-voting explictely as Internet voting: other means of the electronic voting like a punch-card, optical scan ballot etc have never been seriously considered, therefore not known by the public. So the use of the notion "i-voting" would cause confusion.
[3] See about the genesis of the Estonian e-voting project in: [DM04]

- Possible lack of legitimacy of the election results because of following:

    - The individual e-voting procedure can not be supervised by authorities or observed in a traditional way, therefore massive buying and selling of the votes as well exercise of other influence or pressure on the voter are possible;

    - E-voting results can not be verified by the people themselves, and people need to have an absolute faith in the accuracy, honesty and security of the whole electoral apparatus (people, software, hardware). Thus, for people who didn't program the system, the operations of the computers can truly be verified only by knowing the input and comparing the expected output with the actual outcome. Under a secret ballot system, there is no known input, nor is there any expected output with which to compare electoral results.

Certainly it is important to realize, that legitimacy of e-voting or the elections results in whole can be challenged for purely political or personal reasons by some politicians, cryptographs or other opinion leaders without any objective cause.

2.1 Technological point of view

Risks of e-voting must be analyzed from different viewpoints, starting from the general public level and proceeding to more technical issues. There are a large variety of risks on each level; in this paper we will focus on the most principal and important ones. From the general public viewpoint, the major risks of e-voting include the following:

- Incorrectness or untrustworthiness of the voting results, which remain unnoticed at the time of elections (for example, voters are illegitimately influenced, multiple votes from one person are counted, a wrong vote is counted and so on).

- Breach of the voter's anonymity (for example, a person's political preferences will be presented to the general public).

- Annulment of the elections, interruption of the voting process (for example, due to a major security breach in e-voting).

From these three risks, the first two are the most serious. Annulment of the elections may be expensive, but tends to be politically less sensitive.

On the technical level these major risks are especially critical due to three principal problems of e-voting. Historically, one of the primary arguments has been that the security requirements of e-voting are extremely difficult to satisfy due to the conflicting requirements of confidentiality and auditability. The confidentiality requirement states that votes must remain anonymous; the auditability requirement - that every action in the system must be recorded.

A major argument against Internet e-voting states that Internet is an inherently insecure platform. Indeed, various attacks including worms, viruses, spy ware, spoofing, denial of service and others, can be used to compromise the voting results, to break the voter's anonymity, or to interrupt the elections. The vulnerabilities behind these attacks arise from the fundamental properties of the architecture of Internet and current personal computers. It has also been noted that (seemingly) successful e-voting trials do not really prove security of Internet voting. First, it is very difficult to prove that no security breach has occurred; and second, successful trials cannot eliminate security risks for future elections.

Finally, due to these and other problems the e-voting is sometimes argued to be not cost-effective: security measures complicate the election process and the small number of e-voters does not justify the additional costs resulting from this complexity.

2.1 Legal point of view

According to the Estonian Constitution members of the *Riigikogu* as well local government councils shall be elected in free elections based on the principle of proportionality, elections shall be general, equal and direct, and voting shall be secret. There is no special regulation for e-voting in the constitution. It is absolutely clear, that remote Internet voting makes it impossible, to guarantee privacy by the voting act. On the other hand, the required principle of uniformity gives rise to questions about equal access to participate in the voting process and additionally general equality issues.

3 Experience

3.1 Legal solutions

The principle of secrecy consists of the sub-principle of privacy and anonymity (secrecy of the election decision). Remote Internet voting requires in the first line rethinking of the principle of privacy. Voting in privacy should not be regarded as an aim by itself. The principle of secrecy, and its sub-principle of privacy, is there to protect an individual from any pressure or influence against her or his free expression of political preference. So it is a mean for guaranteeing freedom of choice. Such teleological approach to the constitution was the basis of the e-voting provisions from the very beginning of the whole project. [DM02] If we can not use compulsory privacy for guaranteeing the principle of freedom to vote, we must find an another method. The Estonian election law gives the e-voter the right to alter the vote given by electronic means with another e-vote or paper-ballot whereby the paper-ballot has priority. So a “virtual polling booth” is created: the e-voter can choose the moment, when she or he is alone, free of any possible pressure. On the other hand it is an efficient instrument against purchasing of votes. The e-voters possibility to change their e-vote reduces the motivation to exercise any influence or pressure including offer money or goods for any votes.

In Estonia, other that in some countries, the fact whether a person entitled to vote did participate in voting or not, is not regarded as a part of the principle of secrecy. The voter lists that contain information about participation and chosen voting method are preserved in the archive and can be used for research purposes. Researchers have made use of this possibility; incl for the e-voting survey, what unfortunately weakened somewhat the public trust against e-voting. The fact that the official questioner had knowledge about the actual fact of e-voting made some people suspect about the secrecy of their voting decision. These suspicions were leaked in public media but they were more or less kept unmarked. The explanation was that voters' lists have always had according information about who participated and what voting method was used. The voting decision itself has always been secret.

Some months before the municipal elections 2005 the President of Estonia brought e-voting provisions to the Supreme Court for constitutional review arguing that the possibility to change e-votes gives advantages to e-voters in comparison to non-e-voters. E-voters can change their vote for an unlimited number of times but only during e-voting and advance poll days (from sixth to fourth day before actual voting day, i.e. from Monday to Wednesday). The initial version of the e-voting law contained the possibility to change the e-vote with a paper-ballot on the actual voting day. This provision was left out of the law, because this could have given real advantage to e-voters: they would have had the chance to change their election preference on Sunday after receiving additional information about candidates in the second half of the week. After this change all voters who use advance poll possibilities are formally in the same conditions.

The Supreme Court Chamber of Constitutional Review pointed out that despite the repeated electronic voting the voter has no possibility to affect the voting results to a greater degree than those voters who use other voting methods. From the point of view of the voting results this vote is in no way more influential than the votes given by paper ballot. According to the Estonian Election law[4] each voter shall have one vote. When a voter has given several votes electronically, the last vote shall be taken into account. If a voter has voted both electronically and by a ballot paper, the ballot paper shall be taken into account. Within the system of electronic voting the taking only one vote per voter into account is guaranteed by a system similar to the so called system of two envelopes, used upon voting outside the polling station of one's residence during advance poll days.

Upon voting by electronic means a voter makes her or his choice, which shall be encoded (placed in a so-called virtual inner envelope). Thereafter the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote (so-called outer envelope). The personal data and the encoded vote shall be stored together until the counting of votes on the Election Day, with the aim of ascertaining that the person has given only one vote.

[4] See the e-voting provisions in [MVM06]

The personal data of a voter and the vote given by the voter shall be separated after the fact that the voter has given only one vote has been checked and repeated votes have been eliminated. It is possible to open the so-called inner envelope only after the personal data added to the encoded vote have been separated with the help of a key given only to the members of the National Electoral Committee, after the polling stations have been closed. Thus, the system of electronic voting guarantees that only one vote per voter shall be taken into account, ensuring, at the same time, that the voting decision remains secret.

Pursuant to the petition of the President the violation of uniformity of voting also consists of the fact that through the possibility to change the e-vote given for unlimited number of times gives advantage to the e-voters in comparison to other voters; That because other voters do not have the possibility to change their vote. The Chamber said that this interpretation renders the principle of uniform elections a special case of general right to equality. In the legal sense e-voting is equally accessible to all voters. The ID-card necessary for e-voting is mandatory for all inhabitants of Estonia, thus, the state has created no legal obstacles to anyone to e-voting, including to changing one's vote during the advance poll days. It is a fact, that due to factual inequality the possibility to change one's vote through e-voting is not accessible to all voters can be regarded as an infringement of the general right to equality and the principle of uniformity. The principle of equal treatment in the context of electing representative bodies does not mean that absolutely equal possibilities for performing the voting act in equal manner should be guaranteed to all persons entitled to vote. In fact those who use different voting methods provided by law[5] are in different situations. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the Constitution. The aim to increase voter turnout is without any doubt legitimate. The measures the state takes for ensuring the possibility to vote for as many voters as possible are justified and advisable. Another aim of allowing e-voting is the modernization of voting practices what coincides with the aims of e-voting listed in the Recommendation (2004)11 "Legal, operational and technical standards for e-voting" of the Council of Europe.

In accordance with the Penal Code, preventing a person to freely exercise his or her right to elect or be elected at an election or to vote at a referendum, if such prevention involves violence, deceit or threat or takes advantage of a service, economic or other dependent relationship of the person with the offender is punishable by a pecuniary punishment or up to one year of imprisonment. The voter's possibility to change the vote given by electronic means, during the advance polling days, constitutes an essential supplementary guarantee to the observance of the principle of free elections and secret voting upon voting by electronic means.

---

[5]The voting methods allowed in Estonia are: advance poll with paper ballot in- and outside of the polling station of voters' place of permanent residence from 13th to 4th day prior election day; postal voting from abroad; voting at the Estonian Embassies in foreign states; home voting on election day; voting in custodial institutions and hospitals; voting on an Estonian ship, electronic voting from 6th to 4th day before election day and voting with paper-ballot on election day. At local elections not all of them are allowed.

A voter who has been illegally influenced or watched in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again either electronically or by a ballot paper, after having been freed from the influences. In addition to the possibility of subsequently rectifying the vote given under influence, the possibility of voting again serves an important preventive function. When the law guarantees a voter, voting electronically, the possibility to change the vote given by electronic means, the motivation to influence him or her illegally decreases. There are no other equally effective measures, beside the possibility to change the vote given by electronic means, to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium. The infringement of the right to equality and of uniformity, which the possibility of e-voters to change their votes for unlimited number of times can be regarded as amounting to, is not sufficiently intensive to overweigh the aim of increasing the participation in elections and introducing new technological solutions.[6]

3.2 Did voters' turnout increase?

It is very difficult to measure, whether e-voting did influence actual participation rate. Analysis based on facts is impossible; the only way is to question voters and non-voters, especially e-voters whether they had cast their e-vote if the possibility to e-vote would not have existed. E-voting at local government council elections started on 10 October 2005 at 9 am and ended on 12 October 2005 at 8 pm on the web page www.valimised.ee. The e-voting turnout was ~2 % of actual voters, what was estimated as a good result. The research confirms that e-voting will probably not bring those people who principally do not participate to vote. If e-voting does increase turnout then only within those groups of voters, who sometimes vote and sometimes not.

According to the subjective estimation of participation in the absence of e-voting, 4,9% of the questioned e-voters gave the answer that they would certainly not have voted if e-voting would not have been offered; 13,6% gave the answer "probably would not have" [BT06]. According to the proportion of those, who vote in some elections or from time to time, among e-voters and voters at polling station, we see, that 29,2% of e-voters and 21,5% of voters voting at polling station belong to that group [BT06]. So, slight increase of turnout may still be possible. Postal voting is not allowed at local elections. Therefore it is possible, that some Estonian inhabitants living or working in foreign countries could have cast their vote only because e-voting was offered. According factual data unfortunately does not exist.

[6] Decision Nr 3-4-1-13-05 from 1. September 2005 of the Chamber of Constitutional Review of the Estonian Supreme Court. Resume in English in: [MVM06]

The number of persons eligible to vote	1.059.292
The number of votes:	502.479
Valid (incl e-votes)	496.345
Invalid	6.134
Turnout	47%
Total number of e-votes	9.681
The number / of amended repeat e-votes (more than 1 vote per voter)	364
The number of e-voters	9.317
The number of e-votes eligible for counting	9.287
The number of annulled e-votes	30
The % of e-votes amongst all votes	1,87%
% of voters who voted during pre-voting days (incl e-voters)	12%
% of e-voters among all voters who voted during pre-voting days	7%
The number of voters who used ID-card electronically for the first time (for e-voting)	5.774
The % of those, who used ID card for the first time electronically among all e-voters	61%

Figure 1: General statistics of local government elections 2005
(data: National Electoral Committee)[7]

Most popular e-voting times were in the very beginning and in the very end of the e-voting period: in the morning at 9 and in the evening at 19 (probably at the time when people got to their workplace or in the evening at home). During the whole e-voting period, the number of e-voters was the largest at the beginning of the voting period and even larger during the very last hour of e-voting [MVM06]. Most e-votes were given at home (according to the survey 54,5 %); 36,6 % at workplace; 3,6 % at a friends place, cybercafé etc; 3,2 % at a public Internet access point and 1,9 % at the bank office [BT06]. The question, whether the fact that one's colleagues participate in e-voting does or doesn't motivate choosing e-voting or influence participation in general and whether it is good or bad for democracy, needs some further research.

	Women	**%**	**Men**	**%**
up to 29	1062	25,0	1512	30,0
30 - 34	542	12,8	908	18,0
35 - 39	506	11,9	688	13,6
40 - 44	497	11,7	553	11,0
45 - 49	451	10,6	433	8,6
50 - 54	362	8,5	345	6,8
55 - 59	278	6,5	228	4,5
over 60	547	12,9	375	7,4
TOTAL	**4245**	**100,0**	**5042**	**100,0**

Figure 2. Factual statistics about e-voters by age groups and gender

[7] More statistics at the National Electoral Committee web page: http://www.vvk.ee/english/results.pdf [accessed on 01-05-2006]

3.3 Non-discriminatory Access to the voting

The facts we do have, as well the results of surveys show that at the 2005 elections the problem of inequality in gaining representation because of e-voting did not exist. We are in the opinion that the digital gap increases social disparity in elections in today situation only if the number of voting stations decreases or the voting period will be abbreviated. Neither one nor another was the case by elections 2005. The principles of fair elections require formal equality of voting conditions, not material equality. It is generally impossible to guarantee strictly equal conditions for all voters: e.g. the polling station is for some people closer than to another. Therefore, the creation of new and more comfortable voting possibilities does not contradict to the constitutional principles of voting until we do not worsen the "old-fashioned" voting conditions. The most important reasons for not using e-voting were the absence of the Internet access and lack of computer knowledge (according to the survey 67,1 %). Approximately one-fifth of the questioned non-e-voters pointed out that a reason for not e-voting was the sufficiency of the paper-ballot system. Lack of trust with 3,2% and absurdity of e-voting with 1,9% were no dominant reasons [BT06]. Prior to the actual e-voting there was a concern that the possibility to change the e-vote is going to be misused. It was not the case. The general statistics shows that the number of amended e-votes was only 364 (see figure 1), including repeated votes given for demonstration by the members of the e-voting organizing-team. Gender is not an important factor when choosing e-voting from possible voting channels, age on the contrary is quite an important factor: most e-voters belong to the age group 18-29 (see figure 2). It is important to remark, that these age groups are not easily comparable: the age group of 18-29 is much bigger than the group of 30-34 etc.

The hypothesis that e-voting rewards advantages to urban electorate found no proof (see figure 3). When we look at the absolute number of e-voters by towns and rural municipalities, we can see that the largest number of e-votes was given in Estonian capital city Tallinn and in the second-large city Tartu. When we compare the percentage of e-votes with all votes cast in a municipality or town, it can be seen that at the top there is not Tallinn or Tartu but a tiny municipality, the island Ruhnu with 11.1%; neighboring municipalities of the capital city follow with ~4%. Tallinn ranks 15th and Tartu 29th, respectively with 2.75% and 2.42% of all votes. If we compare the percentage of towns and municipalities, the differences are not really great, with the exception of the county near the eastern border with Russian-speaking inhabitants. The exact reasons of e-voting turnout being so low in that area needs further research.

Among 240 districts, there were only 18 with no e-voters at all.

Type of settlement	**Type of political participation**			
	no vote	vote at polling station	e-vote	Total
Urban	67,9%	67,6%	70,2%	68,6%
Rural	32,1%	32,4%	29,8%	31,4%
Total *№ of respondents*	100,0% (305)	100,0% (318)	100,0% (315)	100,0% (938)

Figure 3. Frequency of Political Participation and Mode of Vote in 2005 [BT06]

3.4 Political effects

The initiator of the e-voting project *Reformierakond* (Reform Party) received the most e-votes (32,7 % of all e-votes; the percentage of e-votes in all votes given to Reform Party is 3,61), all other parties supporting e-voting did also well (respective percentages by Pro Patria 17,5 and 3,82; Res Publica 10,4 and 2,29; Social Democrats 9,9 and 2,86). Among other things the Reform Party organized ID-card user trainings and handed out complimentary smart-card readers during their election campaign. Parties who challenged the e-voting until the actual voting time *Keskerakond* (Center Party) and *Rahvaliit* (Peoples Union) received quite few e-votes (8,7 % of all e-votes; the percentage of e-votes in all votes given to Center Party is 0,63; respective percentages by Peoples Union 6,9 and 1,03). Important reason for that can be the opposition towards e-voting among their supporters. The Centre Party who on the background of their general success could have received many e-votes ranked only 5th among the political parties by the number of e-votes. [MVM06]

Prof A. Trechsel and F. Breuer assessed the possible political impact of e-voting using the results of the telephone survey and concluded political neutrality of e-voting (see figure 4).

Independent variables	**B**	**s.e.**	**sig.**
Age	0,267	0,116	0,022
Gender	0,415	0,287	0,148
Settlement	0,361	0,316	0,254
Education	0,289	0,181	0,111
Income	-0,166	0,136	0,221
Language	**-1,377**	**0,546**	**0,012**
Left-right scale	-0,008	0,073	0,908
Political discussions	0,270	0,162	0,095
Trust in Parliament/government	-0,265	0,342	0,438
Trust in politicians	0,188	0,316	0,551
Trust in the State	0,516	0,278	0,064
Computing knowledge	**-0,410**	**0,181**	**0,023**
Frequency of internet use	0,153	0,082	0,063
Location of internet access	0,247	0,172	0,150
Trust in transactions on the internet	-0,325	0,229	0,156
Trust in the procedure of e-voting	**-1,684**	**0,244**	**0,000**
Constant	1,004	1,723	0,560

Figure 4. Multi-variate global model of the impact of socio-demographic and –economic, political and ICT variables on choosing e-voting over voting at the polling stations (logistic regression coefficients). [BT06]

3.5 Technical and Organizational Measures used to ensure security and trustworthiness of e-voting

The organizational issues involve many different aspects. The overall organization of elections, including preparation of initial data, timing of e-voting, collection of results, handling (multiple) e-votes, and other, must support e-voting processes adequately. In spite of somewhat virtual character of the e-voting organization that may not be easy to define and protect from the information security viewpoint, its actors, roles, and responsibilities must be defined, assigned, and managed. In Estonian case, the organizational procedures, including risk management, security procedures, and security awareness activities, were be clearly defined. All e-voting procedures were identified; critical procedures that can lead to major risks were documented and audited by an accredited IT auditor.

The e-voting system was designed to deal with conflicting requirements of confidentiality and auditability. The concept of "digital double-envelope" was used [GD05]. According to it, e-voting should be in a sense analogous to voting with envelopes at a traditional voting (paper-ballot given outside home voting station of the voter and postal voting from abroad). Implementation of this concept may include representation of the inner envelope by an encrypted vote and the outer envelope - by a digital signature.

The e-voting system is managed on several levels: software development and modification, installation and initiation, the active e-voting and subsequent activities. Relevant risk management, configuration management, change management, contingency planning, disaster recovery planning, safeguard selection and implementation and follow up procedures were defined and implemented. System and network monitoring was performed by different parties on different levels during the e-voting period on a 24h basis. All major e-service providers (e.g. banks) and Internet operators were involved in the process with monitoring the overall “health” of Internet – network traffic loads, analysis of possible Trojans/viruses etc.

As of result – no serious attacks occurred and the system was stable. Counting of e-votes was a semi-open procedure with presence of more than 60 international observers, journalists, IT auditors and members of the National Electoral Committee.

4 Conclusion

Estonian e-voting experience seems to prove that it is possible to solve the legal as well technological obstacles. The compulsory ID card with remote identification and digital signature functions as well IT auditors as the guarantee of public trust play a crucial role in the successful experience. The system of e-voting has worked perfectly, all procedures have been legitimate and performed lawfully (respective confirmation of auditors is available).

The attitude to the e-voting of the Estonian public was and is positive[8]. There were no court cases and we do not have any information about purchase of e-votes (on the contrary to the votes on paper-ballot). Here we should underline again, that voting in privacy in the remote unsupervised Internet voting context is a right, not a duty.

The legality and legitimacy of the whole election process has not been questioned for political reasons. One of possible explanations for that can be the public debate about the concept of the Principles of Honest E-Voting[9], what should be certainly continued. The principles of uniformity and generality in their conjunction require that the participation in voting, guaranteed to voters, is as convenient as possible. New voting channels, incl. e-voting serve the aim of increasing the participation in voting and thus protecting the representative nature of representative bodies. E-voting does not change the voting behavior of those persons who principally do not vote in elections, but it accords participation opportunity to the people who have no time or commitment to go to the voting station. Due to several new comfortable voting methods incl. postal voting and advance poll the traditional significance of the Election Day as voting day is anyway gone.

Literature

[BT06] Breuer, F.; Trechsel, A.H. Report for the Council of Europe. E-voting in the 2005 local elections in Estonia. European University Institute. Project leaders Prof.Dr. Alexander H. Trechsel, European University Institute, Florence, Italy & Director of the e-Democracy Centre (e-DC), University of Geneva, Switzerland; Ivar Tallo, Director of the e-Governance Academy, Tallinn, Estonia. Florence, 06.03.2006.

[DM02] Drechsler, W.; Madise, Ü. E-voting in Estonia. – TRAMES 2002, 3, vol 6 (56/51).

[DM04] Drechsler, W.; Madise, Ü. "Electronic Voting in Estonia." In Norbert Kersting and Harald Baldersheim, eds. Electronic Voting and Democracy. A Comparative Analysis. Basingstoke: Palgrave Macmillan, 2004, p 97-108.

[MVM06] Madise, Ü.; Vinkel, P.; Maaten, E. Internet Voting at the Elections of Local Government Councils on 16 October 2005: Report. http://www.vvk.ee/english/report2006.pdf [accessed on 28.04.2006]

[GD05] Estonian e-voting system - General description http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf [accessed on 28.04.2006]

[8] Survey "e-voting and decreasing of political alienation". Faktum, December 2003;
Survey „The attitude of Estonian inhabitants toward e-voting", Faktum, February 2004;
Survey „The attitude of Estonian inhabitants toward e-voting", Faktum, February 2005;
E-voting Survey. Turu-uuringute AS, May - June 2005; Survey "Democracy and national interests". Faktum. October - November 2005.

[9] Available on the e-Governance Academy (eGA) web page: http://www.ega.ee/ [accessed on 28.04.2006]

Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed

Dr. Nadja Braun, Daniel Brändli[1]

Swiss Federal Chancellery
Political Rights Section
Bundeshaus West
3003 Bern, Switzerland
{nadja.braun | daniel.braendli}@bk.admin.ch

Abstract: In Switzerland the Federal Chancellery in cooperation with three cantons has carried out since 2003 a number of pilot trials with the aim of evaluating the feasibility of remote e-voting. Based on a legal basis respecting the council of europe's recommendations five pilot trials have been authorized at national referendums in 2004 and 2005. The pilot trials were evaluated for a number of different aspects, including the potential of e-voting to increase voter turnout, the security risks and its cost-effectiveness. The evaluation has shown that e-voting is feasible in Switzerland. The decision on how to proceed now rests with the Federal Council and the Parliament.

1 Introduction

At the request of the Federal Council and the Parliament and in cooperation with the cantons of Geneva, Neuenburg and Zürich, the Federal Chancellery has carried out a number of pilot trials over the last five years with the aim of evaluating the feasibility of e-voting in Switzerland[2].

In Switzerland, the terms "e-voting" or "vote électronique" are understood to refer primarily to so-called "remote e-voting"[3] – the casting of ones vote via the Internet, by SMS or by other electronic data transmission media. In direct-democratic Switzerland, e-voting is meant to include not only the casting of votes in elections and referendums, but ultimately also the giving of 'electronic signatures' for initiatives, referendums and proposals for candidates for membership of the National Council.

[1] The opinions expressed in this paper do not represent any official statement.
[2] The first milestone within this pilot phase was established by the report [B02] of 09.01.2002.
[3] The same procedure i.e. the casting of a vote elsewhere than in a polling station, is also referred to as "remote internet voting" or "remote voting by electronic means (RVEM)".

The pilot studies of recent years were restricted to voting in elections and referendums, as electronic signature might possibly require an officially recognized digital signature to enable positive identification of the signatory. To date, however, suitably approved digital signatures have not been sufficiently widely used in Switzerland[4].

The following two chapters give, firstly, an outline of the pilot studies and, secondly, a presentation of the major results of the evaluation[5].

2 Pilot Trials

2.1 Preconditions for pilot trials in Switzerland

The legal basis for the legally binding use of e-voting was created on 21st June 2002 within the context of a partial revision of the federal law of 17th December 1976 on political rights (BPR, SR 161.1)[6]. This legislation allows the Federal Council, in consultation with interested cantons and municipalities, to authorize pilot trials which are limited as to place, time and subject matter. A special requirement is that strict control of eligibility to vote, the secrecy of voting and the recording of all votes must be guaranteed. The trials must not be open to misuse. The rules of implementation (Art. 271-27q of the ordinance of 24th May 1978 on political rights, VPR, SR 161.11) set out the preconditions which must be fulfilled before the Federal Council can approve pilot trials of e-voting[7]. The rules of implementation likewise place special emphasis on ensuring security, protecting the secrecy of the vote, checking voter eligibility and preventing the casting of multiple votes.

In implementing the pilot projects, attention was also paid to the *recommendations of the Council of Europe*, in addition to the Swiss legal provisions [C04]. The core message of the CoE recommendation is that e-voting must respect all the principles of democratic voting, and must be as reliable and secure as non-electronic voting. In the recommendation, special emphasis is placed on there being a high level of security, on the characterization of e-voting as an additional form of voting and on the neutrality of the technology. These keynotes are fully endorsed in Switzerland.

---

[4] As of 1st January 2005 (Federal Law on electronic signature, ZertES, SR 943.03), the legal basis for binding transactions is in place.

[5] Publication of the evaluation in the form of a report of the Federal Council for the attention of the Parliament is planned for summer 2006.

[6] Art. 5 § 3, Clause 2, Art. 8*a,* Art. 12 § 3, Art. 38 § 5 and Art. 49 § 3 BPR plus Art. 1 § 1, Clause 2 Federal Law of 19.12.1975 on the political rights of Swiss living abroad (BPRAS, SR *161.5*).

[7] Cf. also the Federal Council directives to the cantons in the circular of 20.09.2002 regarding the application of these rules of implementation (Federal Gazette *2002* 6603-6609).

The *authorization of pilot projects* relating to national ballots is the responsibility of the Federal Council. In order to lessen risks, the Federal Council can limit the scope of the pilot project in respect of place, time and subject-matter. The conditions detailed in the Swiss ordinance on political rights must be observed cumulatively, unless the directive explicitly states otherwise. Any planned use of e-voting at the national level must be authorized in advance by the Federal Council. The cantons had to include detailed technical documentation in their requests for such authorization. Before the first trial, the three pilot systems were checked by professional outside companies engaged by the Federal Chancellery, to ensure that the systems were secure and hacker-proof.

An extremely important precondition for e-voting is the *standardization of the registers of voters*, which are normally kept by the communes. In developing their systems, the pilot cantons were able to refer in part to cantonal regulations, and in part to an agreed standard developed by the eCH association [E04, cf. also B05]. Individual cantonal or communal identifiers were used for personal identification in each case. Due to the lack of unambiguous numerical identification, no cross-cantonal exchange of data between the different voter registers was possible.

In order to preserve the secrecy of the vote, all personal data (name, address, date of birth etc.) were anonymized after the individual voting permits had been generated. The unique voting permit number could then be used to check (against the voting register) whether an individual had already voted, thus ruling out the possibility of multiple voting.

2.2 Pilot trials at national referendums in 2004 and 2005

In 2004 and 2005, a total of five e-voting pilot trials were carried out in the cantons of Geneva, Neuenburg and Zürich on the occasion of national referendums (cf. Table 1). Without exception, all five trials proceeded successfully and without mishap. Prior to the first official use, each of the three electronic voting systems was subjected to an extensive test run overseen by independent experts.

Date	Canton/Communes	Extent of trial	Number of electronic votes (share of all votes as %)
26.09.2004	Geneva: Anières, Carouge, Cologny, Meyrin	22.137 eligible voters	2.723 (21,8%)
28.11.2004	Geneva: Anières, Carouge, Cologny, Collonge-Bellerive, Meyrin, Onex, Vandoeuvres, Versoix	41.431 eligible voters	3.755 (22,4%)
25.09.2005	Neuenburg	1.732 eligible voters*	1.178 (68,0%)
27.11.2005	Zürich: Bertschikon, Bülach, Schlieren	16.726 eligible voters	1.154 (22,1%) (of which 243 by text message)
27.11.2005	Neuenburg	2.469 eligible voters*	1.345 (55,1%)

Table 1: Pilot trials carried out at national referendums

3 Evaluation of the Pilot Trials

The pilot trials were evaluated for a number of different aspects, including the potential of e-voting to increase voter turnout (3.1), the security risks (3.2) and its cost-effectiveness (3.3). These three aspects of the evaluation are summarized below.

3.1 Benefits to and effects on direct democracy

An important argument which is repeatedly raised in favor of e-voting is its potential to increase voter turnout. It is argued that certain groups – young people, on account of their increased use of the Internet; older people, because of their limited mobility; Swiss citizens living abroad, because of lengthy international mail delivery times; blind or partially-sighted persons – would make more frequent use of their voting rights if e-voting were in place.

* Users of the official "Guichet unique" electronic office

In 2004, the Federal Chancellery commissioned the research institute gfs.bern to undertake an empirical study on the potential effect of e-voting on voters across Switzerland [G05][8]. Two-thirds of the eligible voters currently have access to the Internet. The percentage is even higher for younger voters and those who are better educated. The survey revealed that 54% of those asked could imagine using e-voting. The most common reason given for readiness to use e-voting was its user-friendliness. Fears about data security were expressed most strongly by people who will probably not use e-voting.

"Assuming that you were already able to vote electronically, is it highly likely, very likely, fairly unlikely or highly unlikely that you would cast your vote electronically?"

© gfs.bern, Electronic Vote, 2003/2004 (N=4.018)

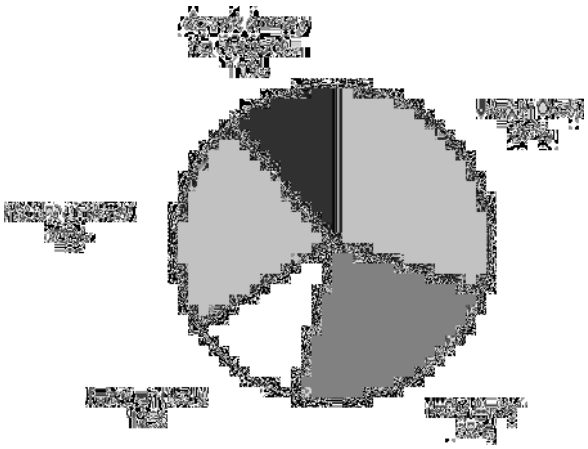


Figure 1: The potential effect of e-voting on Swiss voters

The use of e-voting was not only dependent on a person having available access to the Internet, but also on whether those asked make regular use of this medium for their professional and/or private affairs. Well-educated young males living in urban areas showed the greatest level of interest in e-voting. But the potential is greater than 50% even in the 40-65 age-group of voters and for people from the middle classes.

[8] The studies are based on a supplement to four VOX analyses (ex-post analyses of national referendums) from 2003 and 2004. A total of 4,018 Swiss citizens entitled to vote in national elections and referendums were asked for their opinion .

According to the study, e-voting is particularly attractive to people who stated that they did not vote in referendums either “at all” or “only sometimes”. This finding could be an indication either for a replacement by other forms of voting or for a potential increase in turnout. The potential is greater, the higher the level of interest in political issues and in active participation in political debate. Nonetheless, the study comes to the conclusion that e-voting would have no effect on the balance of power between the different political camps.

The Federal Council had as early as 2002 expressed some skepticism towards the estimates of certain experts of a possible increase in voter turnout [B02, p. 654f.]. Even after the completion of the pilot trials and their academic evaluation, it would be right to preserve such skepticism. The study cited here resulted in an unexpectedly high assessment of the potential of e-voting. As with the indications of a potential increase in voter turnout in all three pilot cantons, these findings would have to be corroborated by multiple trials in all three cantons.

3.2 Risks and security measures

Academics and scientists have grappled intensively with the risks of electronic voting, as e-voting has to meet the very highest security requirements [cf. e.g. A04; J04; M02; O02; R02; S04]. The emphasis has been on the dangers of technical manipulation, as well as on the general threat to a democracy posed by technical risks. Most fears concern ways of ensuring the secrecy of the vote [Br05; Mu02]. A major risk concerns the susceptibility to so-called ‘spoofing’. Voters could give their access data and their vote to a bogus Internet site without realizing it. Using the hacked information, unauthorized persons could subsequently submit their own political preferences to the official referendum server. A similar form of attack might consist in hacking unnoticed into the data flow between the official referendum server and the voter and changing the information so as to affect the vote (man-in-the-middle attack). Within company networks (Intranets), system administrators could try to spy on employees as they vote or seek to influence the vote in some way. It might be possible, finally, to use the buffer store of a voting machine to find out how an individual had voted.

Secure e-voting is feasible: the pilot trials have demonstrated this. But ongoing security depends on being able to maintain control of continually changing threats and risks. The necessary security measures cannot be developed and put in place once and for all. Just as the potential sources of danger (hackers, viruses, Trojan Horses etc.) are continually changing, so must the security measures be continually adapted and improved.

Many suitable security measures were tested as part of the pilot trials. It was important to rule out any risks of systematic misuse. As with conventional forms of voting (ballot-box or postal votes), the possibility that with e-voting, too, individual votes may be falsified, blocked or altered, or that a person’s voting behavior might be observed or deduced, can probably never be completely excluded. Everything must, however, be done to prevent the occurrence of any systematic irregularities or abuses [Br05].

The security measures taken during the pilot trials in the cantons of Geneva, Neuenburg and Zürich succeeded in foiling all registered attacks. Independent experts emphasized the efficiency of the security measures undertaken and credited each of the three cantonal systems with an excellent security architecture.

Postal voting is often used as a comparison to assess the risks of e-voting. Parliament demanded of e-voting a similar level of security to that of postal voting. The required benchmark was exceeded in the pilot trials. The following table[9] summarizes the requirements and the measures undertaken deriving from the legal and security considerations and compares them with analogous requirements and measures in respect of postal voting.

E-voting requirements	**Analogy(-ies) with postal voting**	**Measures taken during the pilot trials**
Positive identification: A person taking part in a referendum or an election must be positively identified as the person he/she claims to be.	Eligible voters give a handwritten signature on the voting permit or on the reply envelope. Voting slips are also filled out by hand.	• Individual and secret access code • Validation by indicating date of birth and/or place of birth • Use of digital signatures imaginable (in the future) • Other security queries such as the self-documenting AHV number would, however, be questionable (protection of secrecy of vote)
Authenticity of the e-voting system Voters must know for certain that their vote will be placed in the designated ballot-box and that it will be included in the count.	Postal votes are delivered by the postal service, handed in in person at the local authority office or posted in the community postbox.	• The SSL can be checked by the voter using his/her fingerprint • The authenticity of the server can be checked by means of a response code and/or pictorial symbols.
Single vote: A voter may cast only one vote.	The voting permit is issued only once and according to name. In postal voting, the original voting permit must be sent back in the return envelope. Repeat voting is thus impossible.	• Immediate cancellation of authorization to vote in the voter database, as soon as a vote (electronic or postal) has been registered • Clear signs on the voting envelope (e.g. an unbroken seal over the secret access code) show whether a citizen could have already voted electronically.
Preservation of voting secrecy/data protection: The voting intention of the voter must remain secret.	The completed voting slips reach the municipal offices in a separate sealed envelope. After verifying the signatures, the voting permit and the voting slip must be separated.	• Separate storage of personal data and voter-specific details on separate systems • Constant shuffling of the electronic ballot-box by means of a random generator. This makes it impossible, for example, to deduce the name of a person based on the sequence of votes cast.
Provisions against risks from 'Acts of God': Interference with voting from storms,	Analogous risks also exist for municipal offices/town halls, the special communal postbox, polling stations, postal sorting offices and	• Use of several redundant servers • Housing of servers in high-security buildings (entry control, fire protection, back-up power supply)

[9] The information in the table refers only to the solutions tested so far in Switzerland in the context of the pilot trials and does not claim to be exhaustive. Cf. also [V04, p. 57f.]

E-voting requirements	Analogy(-ies) with postal voting	Measures taken during the pilot trials
power failures, earthquakes etc.	postal delivery services.	
Reproducibility and provability: It must be possible to recount votes when the tally of votes is very close or in the event of an appeal.	Paper votes can always be recounted. Different people can be asked to undertake the recount. If they wish, citizens can be present at the recount (transparency).	• Preparation of conventional and electronic records, which are countersigned by the relevant authorities when the votes are counted • Preparation of a separate data storage medium (CD-ROM containing the data from the electronic ballot-box and all Log files) • The interests of voters are secured by special inspectors selected by the political parties
Trust: The entire procedure must be trustworthy and able to be checked.	Postal voting enjoys a wide measure of trust among the general public.	• Involvement of inspectors in all sensitive processes • Independent checking of the source codes, Open Source method • Disclosure of proprietary applications
Defence against external attack: a) Enduser devices (personal computers, mobile phones): possible interception and altering of the votes e.g. by the use of "Trojan horses".	Voting material is stolen from the eligible voter by removal from the letter-box after delivery. Systematic misuse cannot be excluded if many voters do not vote and do not tear up their voting papers before disposing of them.	• Multiple protection through Firewalls • Code-voting procedure (Zürich SMS, online transmission of the vote as a numerical code) • Use of state-of-the-art virus protection software
b) "Transport" of the vote from the user to the server: possible interception and alteration of the votes (man-in-the-middle attack).	Voting envelopes could fall into the wrong hands or be destroyed if they are removed from the communal postbox or if a postal sack is stolen or lost in transit.	• Encryption of the vote (SSL) • Details of vote transmitted graphically and not as text • All online packets are tested for their integrity using horizontal checksums
c) Platform (core element of an e-voting system): e.g. "Denial-of-service attacks"	Arson attack on the communal postbox. Or the delivery of the votes is impeded or prevented by a breakdown of the postal service. The risk is small, but increases with increasing centralization of postal services.	• Use of several redundant servers • Collaboration with various providers (DNS hacking)

Table 2: E-voting and postal voting: comparison of requirements and security measures

3.3 Cost-effectiveness of e-voting

Despite the need referred to above for e-voting to satisfy the highest security requirements, it must also be so simple to use that it can be used by every eligible voter. The challenge therefore lies in providing the greatest possible degree of security at an affordable price. At the same time, user-friendliness must not be excessively restricted. Postal voting can provide comparisons in this area too.

In its 2002 report, the Federal Council estimated the cost of a nationwide introduction of e-voting, including running costs over a 10-year period, at 400-620 million Swiss francs [B02, p. 685f.]. This summary estimate was reviewed using the data from the pilot trials. The Federal Chancellery tallied the total costs of the pilot projects at the end of 2005. There were also specific cantonal costs which were not borne by the Federal Chancellery (e.g. the cost of extra jobs and staff).

The financial cost for the development and operation of an e-voting system for both elections and referendums can amount to 15 million Swiss francs. The sum includes operating and maintenance costs for ten years, estimated staff and service costs and the amortization of the development costs. Such a system is scaled for a very large canton or for shared operation by several smaller cantons. If we assume that 1 million voters can use the system, the cost per electronic vote would be less than half a Swiss franc.

Assuming that several cantons operate an e-voting system together, and that those processes which are common to all forms of referendum (such as, for example, the printing of the voting permits, the creation of the voting register, the checking of voting rights etc.) feed into a cantonal or supra-cantonal election and referendum system, the implementation of e-voting would be more cost-effective than postal voting.

4 Conclusions

The pilot trials carried out at communal, cantonal and national levels have shown that e-voting is feasible in Switzerland. The pilot systems and the know-how gained by the pilot cantons is available to other interested cantons for the most part free of charge. The pilot cantons and some other cantons are interested in the progressive extension of the pilot trials to encompass the whole canton, and can also imagine extending the system to cover elections as well, if need be. This would require them to follow strategic guidelines laid out by the Federation, as well as federal assistance in the necessary adaptation of the existing legal provisions.

E-voting is a complex system involving many people at several different levels. A step-by-step approach makes it possible to gather experience and apply it to the improvement of electronic voting. Switzerland has approached the subject from the start at a cautious pace. Once the pilot phase was concluded, it was therefore possible to undertake a thorough evaluation of the various developments in the cantons and to point to a possible way forward. It is now for the political sphere to make the decisions as to how to approach the progressive implementation of an e-voting system. A cautious approach is also necessary in order to minimize risks. E-voting has only a chance of being introduced if all those involved – voters, politicians and authorities – have a lasting acceptance of and trust in the new procedures.

The decision on how to proceed now rests with the Federal Council and the Parliament.

References

[A04] Alvarez, R. Michael/Hall, Thad E.: Point, click and vote, Washington 2004.

[B02] Bericht über den Vote électronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte vom 9. Januar 2002 (report of 09.01.2002 on the Opportunities, Risks and Feasibility of the Electronic Exercise of Political Rights), Bundesblatt 2002, S. 645-700 (BBl 2002 645). Available at: www.admin.ch/ch/d/ff/2002/645.pdf.

[B05] Bundesamt für Statistik: Die Harmonisierung amtlicher Personenregister, kantonale und kommunale Einwohnerregister, Amtlicher Katalog der Merkmale (The standardization of official registers of persons, cantonal and communal registers of residents, Official Catalog of Criteria), Neuchâtel 2005. Available at: http://www.bfs.admin.ch/bfs/portal/de/index/infothek/erhebungen__quellen/statistik_und_register/registerharmonisierung/publikationen.Document.65357.html.

[Br05] Braun, Nadja: Stimmgeheimnis (Secrey of the vote), Diss. Bern 2005.

[C04] Council of Europe: Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies. Available at: http://www.coe.int/t/e/integrated_projects/democracy.

[E04] eCH-Standard "0027:Meldeprozesse" (Reporting processes), as of 29.10.2004. Available at: http://www.unisg.ch/org/idt/echweb.nsf/0/D38E4752D42D358AC1256F3C002F6B0A?OpenDocument&lang=de.

[G05] Research institute gfs.bern: "Das Potenzial der elektronischen Stimmabgabe" (The potential of e-voting), study commissioned by the Federal Chancellery, Bern 2005.

[J04] Jefferson, David/Rubin, Aviel D./Simons, Barbara/Wagner, David: Analyzing Internet Voting Security, Communications of the ACM, 47, Nr. 10, 2004, S. 59-64.

[M02] Mitchison, Neil: Protection against "internal" attacks on e-voting systems, in: Muralt Müller, Hanna/Auer, Andreas/Koller, Thomas (eds.): E-Voting. Tagung 2002 für Informatik und Recht, Bern 2003, S. 255-266 German and French only).

[Mu02] Muralt Müller, Hanna und Koller Thomas (eds.), E-Voting, Tagung 2002 für Informatikrecht, Bern 2002.

[O02] Oppliger, Rolf: E-Voting sicherheitstechnisch betrachtet, digma, 4, 2002, S. 184-188.

[R02] Rubin, Aviel D.: Security Considerations for Remote Electronic Voting, Communications of the ACM, 45, 12, 2002, S. 39-44.

[S04] Schryen, Guido: How Security Problems Can Compromise Remote Internet Voting Systems, in: Prosser, Alexander/Krimmer, Robert (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society, Bonn 2004, S. 121-131.

[V04] Der Vote électronique in der Pilotphase, Zwischenbericht der Bundeskanzlei vom 18. August 2004 (E-Voting in the Pilot Phase, interim report of the Federal Chancellery of 18.08.2004). Available at: http://www.admin.ch/ch/d/egov/ve/dokumente/Zwischenbericht.pdf).

Session 2: Social, Technical, and Political Issues of E-Voting

Contributions to traditional electronic voting systems in order to reinforce citizen confidence

Ana Gómez Oliva, Sergio Sánchez García, Emilia Pérez Belleboni

Dpto. de Ingeniería y Arquitecturas Telemáticas (DIATEL)
Universidad Politécnica de Madrid. Ctra. Valencia km. 7. 28031 Madrid. Spain
{agomez | sergio | belleboni}@diatel.upm.es

Abstract: This document provides a general description of the telematic voting scenario designed by the author's research group. This scenario reinforces verification procedures as key elements to achieve full acceptance of the system on the part of voters. To frame this work, a general overview of electronic voting is given and the conditions entailed by these systems are specified.

1 Problems inherent to telematic voting

Since the first experiments in the 1960's with computerized voting until today, in which electronic ballot boxes or Internet voting are being tested, the mass media highlighted a number of experiences around the world under the general concept of *electronic voting*. However, these experiments have involved diverse types of voting systems, where the security guarantees required in authentication processes, voting and tallying are provided in quite diverse forms. In [CGP02] the authors propose a classification of voting systems into several levels of complexity. We can therefore identify two main groups that are relevant to our work: i) Systems that substitute one of the physical components of traditional voting procedures with some type of electronic process (i.e. Direct-Recording Electronic), and ii) those that use telematic networks to link voters to a remote polling station. For the last several years, nearly all governmental action designed to automate voting processes involve policies that fall within the first group, where the electronic ballot box, with or without a ballot, is the most commonly used device in all cases. The experiences of countries like Brazil [Re04] and India [In06] are noteworthy in this regard, particularly the latter, with its hundreds of millions of votes cast confirming the validity of this method.

In the second group, i.e. voting through telematic networks, which we have decided to call **telematic voting**, there have been few experiences with the status of official validity, although numerous proposals or voting schemes have emerged, defining the agents, procedures and security protocols necessary in order to carry out the voting process. In most of these schemes (of which [CC96] [OMA99] and [Ri99] are samples), determination of the security requirements to be met by voting systems has reproduced the guarantees provided by traditional voting processes, as these efforts have focused mainly on ensuring voter anonymity, preventing votes by voters that are either unauthorized or that have already voted and achieving an accurate vote tally. Moreover, since the voter is casting a vote through telematic networks, these voting schemes include cryptographic procedures that prevent votes from being altered or examined during their transmission to the ballot box.

1.1 Common solutions to basic problems

We shall now discuss in detail the problems faced by the designers of any system of telematic voting and the solutions most commonly adopted:

(1) Properly identify voters when casting votes; that is, there should be no usurpation of identity, for here no person can attest to voters' identity as is done at present in traditional voting with members of a polling station. The method for solving this problem is based, in every case, on the existence of a prior offline procedure involving distribution to voters of specific voting credentials that identify the bearer. These credentials today are found in many forms, from the simplest like a secret key to the most sophisticated, like a digital certificate.

(2) Guarantee the anonymity of voters, so that the credential used to validate a vote – and the voter's identity – cannot be associated with the vote cast itself. The most common solution to this problem is to divide the vote casting process into two phases: vote authentication and the voting process itself, so that distinct, unrelated entities will handle these two processes. Typically, the first entity verifies the credentials of the voter and grants permission to vote, while the second recognizes this permission and accepts the vote of the voter. Precautions must be taken to prevent any collusion between the two entities that might allow for establishing a relationship between the voter and the vote.

(3) Prevent voters from voting more than once. The solution to this problem is provided verifying the voter's credential, by simply marking a given credential as already used, with this status checked prior to giving permission to vote.

1.2 Threats posed by the use of computer networks and systems

In addition to the foregoing requirements to be fulfilled by any voting system, telematic voting systems must face specific threats: first, the fact of using communications networks to interconnect voting system devices, (voting sites, remote polling stations, etc) and second, the use of computer systems to cast votes or undertake counting procedures. Either of these conditions makes the following attacks possible:

(1) Attacks on the confidentiality of information and its integrity, making it feasible for an attacker to modify or eliminate votes legitimately cast or to discern their content.

(2) To counteract such attacks on telematic networks, the most advanced voting systems use cryptographic procedures that usually involve the application of ciphering algorithms of public keys and blind signatures to ensure the confidentiality and integrity of data, as well as to provide proof of the effective source of the same.

(3) These threats are compounded by the real possibility that the communications infrastructure could undergo a denial of service attack on voting day and thereby deny voters their legitimate right to vote. This problem is quite difficult to solve if voting is cast from home over the Internet, owing to the open, universal character of the net. Therefore, the usual countermeasures against this threat are based on constraining the scope of exercise of voting rights: voting from only specific places with the use of private virtual networks.

1.3 Telematic voting and alteration of results

Another danger faced by any voting system, whether traditional or not, is the possible alteration of the voting results from within the system itself. That is, when the results published do not truly reflect the votes cast (i.e., an election is rigged). In traditional voting, this risk is offset by the physical existence on paper of votes cast and the use of supervisors that monitor both the voting and tallying processes. However, in telematic voting, this risk is often underestimated, in spite of the fact that studies of the problem [Me01] indicate that one of the factors preventing social acceptance of these systems is the perception by citizens that it is quite easy to modify electronically stored data.

One of the solutions proposed to deal with this problem involves issuance of a receipt that would allow voters to be sure that the vote has been cast as desired. However, the existence of a receipt showing the vote poses the risk of its use as an element of coercion or sale of votes. Thus, alternative solutions have been discussed [Ch04], which in our view are not fully satisfactory, as they offer only an acceptable probability that votes have been included correctly in the tally.

Nevertheless, few voting schemes address the problems inherent in voting through telematic networks that require powerful verification tools to ensure the accuracy of results against possible collusion between system agents, while adding control elements for monitoring the proper execution of the entire voting process.

1.4 Solution proposed

This article proposes a system of telematic voting (called VOTESCRIPT), that reinforces verification processes as a crucial element to achieve full acceptance of the system by voters. Its most noteworthy features are the following:

a) Voting from specific sites (polling stations, kiosks) to avert both denial of service attacks and coercion of voters.

b) Use of a Java Card to store voting software and data related to the voting process. Inclusion of a receipt stored on the card, which is properly protected to prevent its use for coercion or vote selling.

c) Involvement of vote monitors to supervise and attest to the proper functioning of the voting process. The proposed system arises from the experience of this research group in contributing to the development of a theoretical model used by the Spanish Royal Mint to create its own voting system, for which field tests of the prototype were conducted in Ávila (Spain) in 03/2003. Smart cards technology available at that moment did not allow the prototype to fulfil all the specifications included in the theoretical model. Currently, a complete prototype of VOTESCRIPT has been developed making use of Java Cards.

2 Architecture

The VOTESCRIPT system is based on the use of blind signature algorithms as proposed by Chaum [Ch83] and a smart Java Card that would store the voter keys, the vote delivery applet and the voting receipt, among other things. It relies on the voting designs proposed by Fujioka [FOO93] and Cranor [CC96], while substantially improving upon them, as explained below.

2.1 Agents and persons

The communication scenario of VOTESCRIPT involves a set of automatic systems as follows:

(1) Authentication Points (APs). Computers equipped with card readers – but without cryptographic capacities – in which the voter engages in the authentication process.

(2) Ballot Points (BPs). Like the APs, these are computers equipped with card readers, though without cryptographic abilities, in which voters cast votes. A voter can cast a vote in any of the existing BPs.

(3) An Administration System (AS) that could be considered official, which authenticates voters.

(4) Several Intervention Systems (ISs). These are appointed by each of the groupings of electors or the candidacies authorized to supervise voting, with the mission of supplementing the work of the Administration System.

(5) A Ballot Box (BB) that collects votes cast and returns voting receipts.

(6) A Tallier (T), which could be considered official, for tallying votes following the end of the vote reception period. The key is a secret shared between the Administration and the Intervention Systems, and is obtained at the end of the vote reception period.

(7) Several Tally Intervention Systems to supervise the task previously performed by the official Tallier.

(8) Verification Points (VPs) to enable voters to see that their vote has been included and properly accounted for.

(9) A Tally Board that will hold the results published for a short period of time. The key is a secret shared between the administrator and the intervention systems, and is obtained when the individual verification process is performed.

(10) Voters. Each voter has a smart voting card, a Java Card that contains not only cryptographic algorithms specially designed for VOTESCRIPT, but which also executes part of the voter software.

(11) The Election Authority (EA). Consists of a group of persons responsible for general oversight of the system and charged with addressing any complaints.

2.2 Description of protocol

During the voting period, citizens that wish to vote will go through the steps described below, which constitute the VOTESCRIPT protocol (Figure 1).

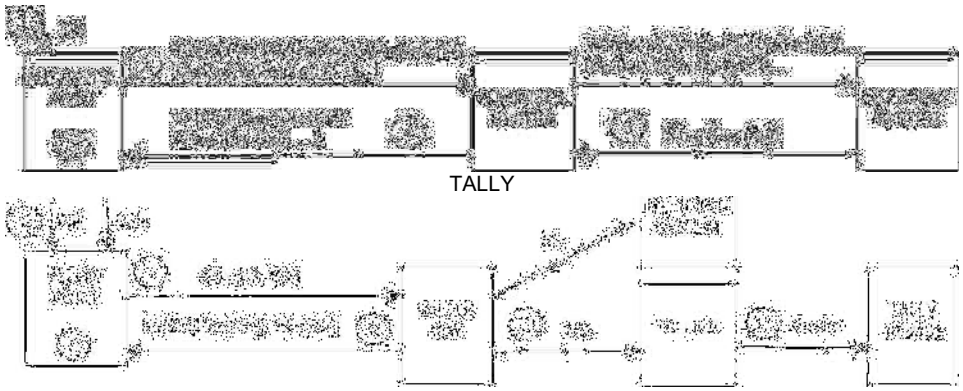


Figure 1: Voting protocol

Voter-Authentication Point Relationship

1 At the Authentication Point, the Voter inserts the Voter Card and is authenticated with a PIN or a biometric mechanism of identification.

2 The Voter Card, which contains two Voter keys – a public and private one – generates a pair of asymmetrical keys for voting (k_{dV}, k_{cV}) and a series of opacity factors. The key k_{dV} is opaque for the Administration System and for each of the Intervention System. The card signs the *voter ID* and all the opaque keys and ciphers the result with the public key of the Administration System. The Authentication Point sends this information to the Administration System.

AS_P [V_s (Voter Id), (O_{AS} (k_{dV}), V_s (O_{AS} (k_{dV})), AS), (O_{IS1} (k_{dV}), V_s (O_{IS1} (k_{dV})), IS 1), ...]

3 The Administration System reads and deciphers the data received and sends all the data to all the Intervention Systems. Each of the Intervention Systems, in the same way as the Administration System, checks that the Id is on the list of valid Ids, that the signature of the Voter making the request is correct and that the card has not undergone authentication previously. If not, the reception is rejected. If everything is in order, the Administration System and each Intervention System blindly signs the relevant opaque k_{dV} key.

4 The entirety of the opaque keys are signed by the Administration System with its private key and ciphered with the voter's public key, and then sent to the Authentication Point.

VP [ASS[ASbsig (OAS (kdV)), IS1bsig (OIS1 (kdV)), ...]]

5 The Authentication Point sends to the Voter Card the data received from the Administration System, so that the smart card receives the k_{dV} signed by the Administration System and by the Intervention Systems. It then verifies that the signatures are correct, and if they are, it stores them, so that they will constitute the vote delivery authorization for the voter during the voting process.

Voter - Ballot Point Relationship

6 At the Ballot Point, the Voter inserts the Card and is authenticated by means of a PIN or a biometric identification mechanism.

7 The Ballot Point asks the Voter to vote. In the Voter Card, the vote chosen is ciphered with k_{cV} and a piece of information is created with the ciphered vote, the k_{dV} and k_{dV} keys signed by the Administration System and the Intervention Systems. Then this piece of information is "stored" in a *T Secure Envelope* between the smart card and the Tallier. A *symmetrical* key (KS) is generated, joined to the T Secure Envelope and stored in a new *Secure Envelope BB*, which is sent to the Ballot Box.

SEBB[KS, SET]

8 The Ballot Box, after eliminating the *Secure Envelope BB* protecting the information received, obtains the *KS* and the *T Secure Envelope*. The Ballot Box stores the *T Secure Envelopes* received until the voting period is over. Based on the data protected with *T Secure Envelope*, it returns a receipt to the Ballot Point that preserves the anonymity of the voter. To generate the receipt, it performs the following operations: a) it ciphers *T Secure Envelope* with the public key of the Election Authority b) it signs it with its private key, and c) ciphers the receipt with the symmetrical key it received from the Ballot Point.

KS[BBs[EAP[SET]], EAP[SET]]

9 In the Voting Booth, information received is delivered to the Voter Card, which obtains the receipt, and it verifies the signature by the Ballot Box. The vote receipt is stored in the Voter Card and only the Electoral Authority can gain access to the data of the receipt in case of a complaint after the end of the voting process.

Opening the Ballot Box and tallying the votes

10 Opening the Ballot Box requires the physical presence of the Administrator and a sufficient number of scrutineers, who will insert their smart cards in the readers and authenticate themselves, either biometrically or with a PIN. The Ballot Box randomizes everything it receives and sends it to the Tallier and the Tally Intervention Systems, while also providing persons with management and supervision responsibilities over the electoral system a list of the data that has been sent. At that moment, all the information received by the Ballot Box during its operations is deleted. The restricted disclosure of the records transferred by the Ballot Box will help verify that the Tallier and the Tallier Intervention Systems are receiving the same information, so as to enable identification any element causing a malfunction in the event an alteration of the vote is detected.

11 The vote tally is then undertaken. Prior to reading the results, the System Administrator and the Scrutineers once again use their smart cards – with a shared secret procedure – to jointly provide the Tallier and the Tally Intervention System their private keys (which are stored and hided until that moment) needed to begin operations. After receiving all the information from the Ballot Box, the Tallier opens the T Secure Envelopes, performs the vote tally and sends to the Tally Board the information, composed of a kdV key and the kdV key signed by the Administration System and the Intervention Systems, along with the deciphered vote. The Tally Board announces the results of the vote to persons with management and supervisory responsibilities over the electoral system.

2.3 Voter Card

Along with the procedures designed to enable audits of software and the results, one of the pillars undergirding the strength of the proposed voting system is the possession of a smart card on the part of each voter. To meet the essential requirements of a voting system the smart card includes self-protection mechanisms against any attempt at reading or writing by equipment that is not standardized for the voting system.

The fact that all citizens make use of a smart card that enables them to sign information to offer proof of origin and decipher confidential information is not sufficient to provide the guarantees required by a voting system. A smart card is needed with cryptographic capacities that have been specially designed for this project, enabling performance of sensitive cryptographic processes, in addition to the usual tasks of identifying its holder. If performed outside the card, these processes would leave a trail of operations in machines that could be subject to subsequent analyses, with the intention of breaking the basic principle of secret voting.

The voter's smart card will internally generate keys for subsequent use. Among these are two pairs of asymmetrical keys: i) one composed of a secret key used to sign or decipher, and another of the public key, which is duly certified and disclosed by the responsible authority, to guarantee the identity of the holder. ii) The other pair is similarly useful to the prior one, but guaranteeing, this time, the anonymity of the holder. Cryptographic mechanisms ensure that the card bearer is a legitimate voter, that two voters will not have the same pair of keys, or that a single voter will not have more than a pair of keys for this use. The cryptographic procedures used will also ensure that no internal or external agent or collusion between them will be capable of disclosing the identity of the voter. This key will be used to legitimate the vote, which will come ciphered from the card so that it can be deciphered only by the Tallier in the tally phase.

Cryptographic processes to be executed inside the card also require the existence of a session key and opacity factors, knowledge of which by third parties would compromise the security of the system to the same extent as if the secret keys were disclosed. Thus, the smart card is the valid secure format, for it will generate keys and factors and, when necessary, share the keys with other agents; it will come from the card with all the confidentiality guarantees offered by cryptographic mechanisms, namely ciphering with the public key of the receiver.

Ciphering with a public key generally offers confidentiality guarantees; however, in voting processes, the number of messages to be ciphered is limited and sheer force may be sufficient to disclose the message. Thus, the card also includes the mechanism of random chains, which must also be generated inside the card, since it is indispensable that the chain be unknown to prevent successful violation of the secret vote.

For the purposes of use following publication of the results, the Ballot Box will give the voter a receipt for the vote. This receipt is designed so as not to expose the voter to the risks of coercion, since it is ciphered with the public key of the Electoral Authority. In this project, the citizen's smart card will securely store the receipt, having first verified its authenticity and storing it in a form that it can be read only by the Electoral Authority.

3 Individual verification and global verification

This project envisages two types of verification of results, which as a whole will act as a deterrent to temptations to commit fraud by the persons responsible for the operations of the different systems, since not only will the malfunction be detected, but also the system in which the malfunction has occurred will be identified unequivocally.

There are two types of verification: global and individual. Global verification of results is undertaken by candidates' representatives or by groupings of electors authorized to perform monitoring of the process. Individual verification is effected by the voter him or herself, with protection against possible coercion by means of properly designed procedures. As already described, the work of the Administrator during the voting process is supervised by the Intervention Systems in such a way that any anomalous issuance or denial of authorizations would be detected.

After the period provided for voters to deliver their votes to the Tallier, the content of the Tallier will be delivered to the Ballot Box and a copy of the data will be received in the Tally Intervention Systems, thus dissuading the Tallier from the intention of eliminating, adding or modifying votes. It would still be possible for the Ballot Box to destroy votes prior to delivering them to the Tallier and the Tally Intervention Systems. This circumstance – apart from raising less interest, since the destruction would be carried out against ciphered pieces of information, the true meaning of which is unknown – would be detected with individual verification procedures by means of the vote receipt signed by the Tallier and stored in the voter's smart card.

3.1 Global verification

Each Scrutineer will have a machine – Tally Intervention System – which will load a copy of the information that the Ballot Box delivers to the Tallier. This machine shall be audited in advance by experts trusted by system managers to achieve complete confidence that it can only perform a vote tally. Any divergence between the votes obtained by the Tally Intervention System and those obtained by the Tallier and published in the Tally Board would be a sign of an anomaly. Thus, neither the Tallier nor the Tally Board can alter – i.e., add, eliminate or modify – votes, nor will they are able to accept the validity of votes that have not been properly authorized. Both for lists of records received by the Tallier and for lists of information delivered to each candidacy, a validity period shall be in effect, so that once the specified time has elapsed and the election is considered valid, the lists must be destroyed in an audited procedure.

3.2 Individual verification

Once voting has concluded and the results have been published, each Voter can independently check that his or her vote has been properly accounted for. This verification is performed by a voter at their own initiative, with resources available to ensure their anonymity and protection from coercion. The Voter need only go to a Verification Point – in an individual manner – use the Voter Card and ask to be shown the vote associated to the information published by the Tallier and the information stored on the card. At this site, the same measures must be taken to ensure that the voter is protected against external surveillance as were taken when casting a vote at the Ballot Point. If the voter does not accept the vote shown at the Ballot Point, the person may appeal to the collegial body called the Electoral Authority, which is responsible for overseeing the proper functioning of the system, and which addresses all complaints lodged by voters. When a complaint is made by a voter regarding treatment of their vote, the Electoral Authority can obtain the vote receipt stored in the smart card of the voter and will use all cryptographic proofs available in the system to investigate the validity of the complaint. The Electoral Authority will obtain solid cryptographic proofs to determine where the anomaly lies and what agent is responsible for it.

4 Innovations of VOTESCRIPT system

This section highlights the main innovations provided by the VOTESCRIPT system, with a comparison of the solutions it proposes with those contained in the main voting schemes used as a reference in this field.

(1) The VOTESCRIPT system provides an individual verification system that enables each voter to check, in specific places and during a determinate period of time, whether their vote has been properly included and accounted for. The innovation as regards other solutions lies in the fact that the process is private, as the voter can at no time show to unauthorized third parties the content of the vote, thus preventing the buying and selling of votes or extortion.

(2) The existence of Intervention System is one of the main innovations of this system, since it enables monitoring of the entire electoral process by groupings of citizens or by duly authorized candidacies. Global verification made available to scrutineers provides solid cryptographic proofs that make it possible to demonstrate unequivocally whether the system has operated fraudulently or not.

(3) The cryptographic cards designed for the project guarantee the identity of the voter, and also perform all functions of ciphering and deciphering, generate of session keys and authentication of signatures in the card itself, with the aim of blocking access to critical information by malicious users. The voter card is a Java Card that contains vote-casting software, while it stores certain information associated to the vote¬casting process, the receipt, with a view to enabling subsequent verification.

(4) There is a collegial body called the Electoral Authority, which is charged with the tasks of overseeing the proper functioning of the system and addressing any complaints made by voters. In the event of a complaint by a voter about the treatment given their vote, the Electoral Authority shall discover and compare all the cryptographic proofs in the system in order to check the validity of the tally.

(5) The system also ensures that the content of a vote cannot be disclosed in the future. Cryptographic presentation of the vote through cryptographic algorithms means that these systems cannot gain knowledge of the vote's content, but it does not ensure that the advancement of cryptoanalysis will not enable it to be known in the future.

5 Conclusions

Today, experiences in telematic voting abound, and these initiatives always highlight the benefit for voters of being able to cast a vote from any computer connected to the Internet. However, the euphoria seen in these experiments makes both organizers and voters overlook the fact that these systems are unable to demonstrate that the results published have not been tampered with prior to their release.

The system presented herein is fully verifiable, as the system's strength lies in its provision of cryptographically solid and secure pieces of information that can be used as proof before third parties in case of litigation or rejection of the results of the process. In the VOTESCRIPT system, as in other recent proposals for telematic voting, the smart card serves as a security token that allows for the protected storing of private keys that enable the voter to undertake authentication in the system and cast a vote in reliable manner. Nevertheless, the smart card plays a much more important role in VOTESCRIPT than these other systems.

The system presented constitutes a valid solution to traditional problems of voting systems, and it can counteract the understandable wariness of voters towards telematic voting processes. E-voting systems that aspire to replace traditional voting systems must include the positive aspects of these traditional arrangements, while offering new functionalities such as those presented here in order to deserve the trust of the citizenry.

References

[CC96] Cranor, Lorrie F.; Cytron, Ronald K.:. Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA, 1996.

[CGP02] Carracedo, J.; Gómez, A.; Moreno, J.; Pérez, E.; Carracedo, J.D.: Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT). II Congreso Iberoamericano de Telemática. CITA'2002. Mérida, Venezuela. 2002.

[Ch04] Chaum, D.: Secret-Ballot Receipts and Transparent Integrity. IEEE Security & Privacy. Vol 2 N1. January-February 2004; pp 38-47.

[Ch83] Chaum, D.: Blind signatures for untraceable payments. Advances in Cryptology, Crypto '82, Springer-Verlag, Berlin. 1983; pp. 199-203.

[In06] Indian Voting. http://www.ensl.cs.gwu.edu/voting/India, last accessed February 2006.

[Me01] Mercuri, R.: Testimony presented to the U.S. House of Representatives Committee on Science. http://www.house.gov/science/full/may22/mercuri.htm. 2001.

[OMA99] Ohkubo, M; Miura, F.: Abe, M.; Fujioka, A.; Okamoto, T.: An Improvement on a Practical Secret Voting Scheme. Lecture Notes in Computer Science 1729, Springer-Verlag, Berlin, 1999; pp. 225-234.

[Re04] Rezende P.: Electronic Voting Systems. Is Brazil ahead of its time?. Cryptobytes, Vol 7, N. 2, RSA Security Laboratories, USA. Fall 2004; pp. 2-8. http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_Fall2004.pdf, last accessed February 2006.

[Ri99] Riera i Jorba, A.: Design of Implementable Solutions for Large Scale Implementable Voting Schemes. PhD thesis, Universitat Antónoma de Barcelona, 1999.

A preliminary question: Is e-voting actually useful for our democratic institutions? What do we need it for?

Jordi Barrat Esteve

Dept. Dret Públic (SEJ2004-03844JURI / LEO26A05)
Universitat Rovira i Virgili
Avda. Catalunya, 35
43002, Tarragona, Catalonia / Spain
jordi.barrat@urv.net

Abstract: The current development of e-voting systems worldwide raises several specific interesting issues from a legal point of view. Auditability measures, identification procedures or guarantees for voting secrecy and equality are good examples, but we often forget a fundamental question: the usefulness of these new technologies. This paper intends to provide an answer that takes into account the complexity of all democratic systems. An updated image of the electoral procedures, the advantages for disabled people, the reduction of economic charges in the electoral fields or the increase of voting turnout will be analysed as the possible positive consequences of e-voting systems.

1 Presentation

The theoretical arguments about e-voting procedures often begin with a couple of general statements that it is worth recalling. First of all, political participation cannot – and should not— remain isolated from the vertiginous development of ICT. In the future, these new technologies will condition, with even greater intensity than nowadays, the ways popular will is expressed and, probably, votes are cast.

On the other hand, fears are also voiced about the dangers of a non-reasonable transformation of political participation channels. New values could appear and the supreme democratic goals could suddenly be found to be secondary to the use of new technological tools. Basic principles, such as equality and freedom, the secrecy of the vote, the consolidation of free public opinion or the existence of enough socialization areas should then not be displaced by other narrow strategies favouring the use of ICT.

It is very difficult to disagree with these obvious statements, but there are others, both positive and negative for e-voting systems, which are too generic. They are very short on analysis and do not take into account the complexity of these technical developments. This paper intends to provide some specific theoretical elements about the role of e-voting procedures in our democratic institutions [for a general overview, see Tu05, Gr03, KB04, PK04 and TM05].

It will not therefore consider such important specific issues as auditability measures for e-voting systems or identification procedures in remote voting. We will remain at a preliminary stage and discuss whether e-voting is actually useful for us.

2 Necessity and usefulness of electronic voting systems

Electoral institutions already accept computer procedures in some processes like the roll out or the transmission of results, but we should try to determine whether these technologies could also be useful tools for casting a vote. The physical identification of a voter, a transparent urn or an isolated booth are main elements in our electoral scheme and we would like to know if they need technical updating, maybe with e-voting solutions, or whether the current structure is better. The answer should not depend only on technological optimism because tools can easily become a goal in themselves and this situation could not be considered as an advantage for the electoral system. The only way to accept these innovations is to prove that they will be useful for citizen participation and, in a more specific way, for the vote casting.

The specific answer will depend on the electoral systems and a variety of parameters should be taken into account. For instance, many political institutions have no important problems and there is no legal or social necessity to make changes. Most European countries follow this model. Electoral discussions focus on the eligibility formula (proportional rules, etc.), but they do not foresee the need to modify electoral procedures that have been tested in several elections and accepted by everybody (I). In these cases, is it actually a priority to introduce e-voting mechanisms? Would they maybe generate inherent dangers that could weaken a popularly accepted system such as the current one?

In our understanding, these are correct and reasonable concerns given that we are dealing with highly sensitive areas in which the expression of the sovereign will is at stake. It would not, therefore, be wise to introduce innovations whose consequences have not been sufficiently analysed and compared. Even so, we believe that there are several reasons for encouraging a slow introduction of electronic voting systems.

It should be noted, in the first instance, that electoral procedures should not be limited to an *outdated technological framework* because it would give our current modern society a poor image. As Michael REMMERT points out «modernising how people vote will not, *per se*, improve democratic participation but failure to do so is likely to weaken the credibility and legitimacy of democratic institutions» [Re03: slide 34]. This initiative, however, cannot ignore the correct functioning of many electoral systems. If REMMERT's statement is understood to be saying that we have no choice to make in electoral modification, that there is an unavoidable necessity to change the current systems by introducing new technologies, it will not be acceptable. I think, however, that REMMERT's quotation can help us if we reduce its sense. Obviously, we should not forget the reasonable results of current elections, but we should always search for innovations that not only maintain the traditional electoral guarantees of any democratic system but also provide other advantages. As REMMERT foresees, our not doing this will probably decrease the system's legitimacy because, although the organization is correct nowadays, efforts must be made to keep the system up to date. Constant awareness must be maintained so that, without endangering the success and stability already reached, electoral processes gradually incorporate the technologies that characterize our era.

On the other hand, the electronic vote can be enormously *useful for certain sectors of society* (for example disabled citizens, absent residents). These are groups that often encounter many problems when it comes to exercising their right to vote, and new technologies, if designed correctly, could facilitate their participation considerably. It would therefore be possible, for both groups, to vote remotely and, in the case of the blind, electronic tools could even allow an autonomous polling-station vote.

The current low turnout of residents living abroad has several explanations, but two of them are, without doubt, the bureaucratic effort they have to make in some cases and the important role of the postal administration of different countries with very narrow deadlines [see Ca03]. Voting from abroad therefore is not simple, but Internet voting could maybe make it much easier.

Disabled citizens could always use these new voting channels. Electronic devices would make it possible for blind people to cast their votes autonomously. Spanish legislation (art. 87LOREG) currently provides disabled voters with the possibility of an assisted vote, but, even though this is a reasonable solution, it is certainly true that e-voting would allow even blind people to make a vote without help and this is obviously a great advantage.

These considerations show that it is important to define the typology of e-voting systems because not all electronic procedures will provide good solutions for disabled people. While the computer- and even mobile-phone applications more easily accept specific devices for disabled people, other e-voting systems, like those based on optical ballots, are considerably less useful from this point of view.

Blind people, for instance, will not be able to use optical ballots because they cannot have audio devices. Printing *braille* ballots could be a solution, though costly, but it is not e-voting. What is more, the separation of paper ballots into Braille and non-Braille could become a serious problem for the secrecy of the vote (see Resolution *Junta Electoral Central* / January 31st 2000; Fu00: 43-44).

In conclusion, the analysis of the usefulness of e-voting procedures should take into account the differences among them because they all have different frameworks.

Thirdly, electronic voting systems are more *versatile and flexible* than anything previously known. Today, the logistics surrounding elections involves economic, time and human costs that make it difficult for them to be conducted frequently. Some electronic voting models –not all– simplify this process and make it possible to imagine a future in which more participation tools could be made available to citizens. It should also be mentioned, not forgetting the important factors regarding security, that a good electronic voting system would be much more exact and precise than the current one. As Andreu RIERA, the person in charge of Scytl pointed out during the presentation of the citizen consultation *MadridParticipa*, there are still «muchos más errores en papel que en formato electrónico» ("many more errors on paper than in electronic format").

However, are these new participation channels actually good? Should we back an electoral system that includes the remote vote from home? Would it be a democratic advantage or a disadvantage? These questions are closely related to the theoretical analysis of democratic representation, which is now experiencing difficult moments. Increasing direct citizen participation could be one solution because it is an attempt to reduce the role of the political parties by empowering citizens with new participation tools.

However, even people who agree with this proposal often stress the dangers of a massive introduction of direct participation tools. Democracy is both casting a vote and having a society with a sensible way of life. It needs to provide citizens with information and create debate among them so that political ideas are to mature sufficiently. To recklessly promote an increasing number of consultations could have negative collateral consequences for the democratic system. And, if this is so, is the convenience of e-voting tools, and the resulting almost effortless multiplication of our voting potential, actually an advantage? Should we consider it to be positive?

Despite all the above, a well-designed democracy based on citizen participation is always a good initiative and, in the future, there will probably be more opportunities within this framework to accept direct and binding citizen consultations. E-voting solutions can facilitate this path as long as they reduce the economic and logistic cost of an election, but this does not automatically mean that they must be massively implemented. There will be the option to do so, but those responsible for the democratic process should evaluate whether it is advisable.

Whatever solution we adopt, there is another issue that is closely related to this one. Many authors think that Internet voting may endanger the public nature of the voting day because the changes in the *electoral routine*, an essential component for any democratic procedure, allow votes to be cast from private places (companies, home, etc.). The political socialization process, then, will be different and it could also generate different and maybe negative political values because there will not be a physical relationship among voters. Following the explanation of Andreas AUER and Alexander TRECHSEL, «le citoyen n'irait plus voter en pensant à l'intérêt général, mais il voterait en tenant compte uniquement de son propre intérêt» [the citizen will not vote considering the general interest, he/she will only consider his/her own interest] (AT01: 45-46; see Su01).

I think however that this strong defence of the current electoral routine is a direct consequence of the system's weaknesses and it should strengthen the need for a democracy with more participation channels. If a short one-day meeting has become an essential component in our democratic behaviour, it is clear that we have a serious problem because the political system is not actually progressing. The relationship between citizens and their representatives cannot be reduced to an occasional point of contact and political socialization should not rely upon this small parameter. It should be a day-to-day process. Within this normal democratic framework, the absence of one act of socialization as a consequence of the introduction of Internet voting should be of no importance and it should be easily accepted.

It should also be noted that there could be virtual socialization areas. New technologies have such interactivity and simultaneity that they can emulate physical meetings and thus create complementary socialization channels. The above-mentioned authors use the following argument to respond to criticism: «il est plus probable que dans le contexte social actuel, une prise de conscience plus compléte des enjeux sociaux d'une votation se fasse à travers les informations et les débats que les citoyens pourront avoir sur Internet avant de voter» [in our current social framework, the use before voting of Internet information and on-line debates will probably generate a more complete idea of the social challenges of an election] (AT01: 46; see KK05).

Anyway, some e-voting procedures do not change the current electoral liturgy. Optical ballots, for instance, are usually presented as mechanisms that do not alter voting behaviour and this is their main advantage. Moreover, both computers and telephone devices can be used in official polling stations, so they will not change the current socialization process during the voting day.

However, the economic advantage of e-voting seems to be linked with the use of non official places for casting a vote because, if we maintain the current network of polling stations, there will be no decrease in logistical obstacles or economic expenses. The possibility of asking citizens for their opinion more frequently also disappears. Optical ballots need the same number of polling stations and they will be more expensive because, even if the current combination of paper and urns is maintained, the ballots contain electronic devices that will probably increase their price.

However, the other e-voting systems, with computers and phones, are not necessarily cheaper. If they are used within official polling stations, our conclusions here are the same as those of the paragraph above. If they are used from other places, the logistical organization could be less, but the final cost will depend on the development of the computer applications and security measures that they need. Both of these situations may be cheaper or more expensive than the current paper ballot system. This depends on the fees determined by the computer experts.

Finally we should note that *election turnout* could increase as a result of implementing electronic procedures. It is frequently mentioned that the use of new technologies would make voting more attractive and certain segments of the population that traditionally abstain, such as young people, may change their attitude with these measures. The fact is, however, that there are no conclusive studies. While some experiences show that the electronic vote increases participation, others indicate the opposite. As a guide, we should mention the tests undertaken during the last Catalan elections in which certain absent residents, among whom were the Catalans living in Mexico, were allowed to use the Internet experimentally to vote. The number of participants exceeded the number of official voters by 226% (see BR04: § 3 / table 3). On the other hand, other experiences show very low rates. For example, in the MadridParticipa citizen Consultation in 2004, only 0.63% of the total electorate took part (see BR04a). The absence of precedents, however, makes it difficult to compare and to conclude whether new technologies encourage more or less participation. There are a number of variables that influence these results (e. g. a consultation is not the same as an election). Nor is it the same if electronic systems act in a unique or complimentary way. Lastly the method used also influences the process: systems based on remote voting in non-controlled environments do not present the same degree of difficulty as models based on optical paper-ballots.

The number of voters is only one parameter, but there are others that also have an important influence on increasing the quality of a democratic system: the *geographic distribution* of votes and the way votes are cast.

The Barcelona Technical Engineering Association (CETIB) is a good example of the first one. Before June 2005 the members of this Association could renew the presidential board every four years by voting through only one channel. There was an official polling station in the Association's main building, in downtown Barcelona, but this electoral organization was disadvantageous for those members who did not live there. For instance, if we analyse the previous results, it is easy to prove that the percentage of Barcelona inhabitants who voted was higher than the percentage of citizens of this city on the census. Neither did total turnout rates ever reach 10% of the electoral roll.

Therefore, in June 2005, the Association's Board decided to accept two voting channels. They intended to increase the total number of voters and also to balance the privileges of some members with a new distribution of votes from a geographical point of view. Each electoral county was to have the same proportion of voters and registered members.

Unfortunately, the turnout decreased in June 2005, but there was significant progress in geographical balancing. As Oriol CISTERÓ'S graphs indicate, the *Barcelonès* County, including the capital Barcelona, decreased from 71 to 64 per cent of the votes cast while its proportion of members was 50% (2005: slide 14).

The second graph, which refers to the e-voting channel is even more significant: if we analyse the geographical distribution of votes, the new balance more accurately reflects the percentage of members. In this case, the *Barcelonès* County represents only 53% of the votes, which is very close to the 50% of registered members living in this electoral district (Ci05: slide 15).

Beside the total turnout and the geographical balancing, another parameter was used to evaluate the success of the e-voting procedures: *the way votes were cast*. The acceptance of electronic means in the General Assemblies of Spanish companies with stockholders is a good example.

The initial situation is very negative because these Assemblies often have a considerable democratic deficit. Most stockholders do not go to the meeting and they delegate their votes. The company admistrators themselves encourage these delegations. Therefore, the company has an internal democratic functioning, but only from a formal point of view. Massive delegations also make the control task that belongs equally to all stockholders more difficult.

In view of this situation and as a result of new corporate governance rules, the Spanish Act 26/2003, about transparency in stockmarkets, added two new paragraphs to article 15 of the Spanish legislation on the companies involved. The first one provides for a vote in the General Assembly cast by electronic means: «de conformidad con lo que se disponga en los estatutos ... podrá delegarse o ejercerse por el accionista mediante correspondencia postal, electrónica o cualquier otro medio de comunicación a distancia» ("in accordance with what is stipulated in the statutes…it may be delegated or executed by the shareholder by postal mail, electronic mail or any other means of remote communication"). This legislation is a direct consequence of the ALDAMA report, the main document produced by a specific Commission created to analyse the transparency and security of the financial markets. Among other issues related to Stockholders Assemblies, this text recommends that e-voting mechanisms be used: «implantar los sistemas necesarios para el cómputo electrónico del quórum, así como para la delegación y el voto por correo o por medios electrónicos» ("to implement the systems required to electronically compute the quorum, and to delegate and vote by mail or electronic means") (In03: 32). There are no other similar Acts in Spain, but VAÑÓ VAÑÓ thinks that this lack does not prevent these electoral procedures from also being included in other financial companies like those based on a collective property of the workers themselves –*credit unions / cooperativas de crédito*— (Va04: 136-137).

Several companies have already modified their internal rules and there have already been the first cases of stockholders voting remotely. The possible simultaneous casting of votes, remotely or traditionally, during the Assembly itself creates considerable technological challenges related to digital identification procedures.

There are also specific rules for delegating the right to vote (see Va05: 225-255). Some pioneer experiences, like Union Fenosa in 2003, had no positive results because only one stockholder finally cast his/her vote (see Va05: 24), but subsequent experiences were successful in consolidating a new democratic framework for these companies.

Shortly, even with the same turnout rates, e-voting procedures can offer other significant advantages like the option of a direct and personal vote. There would be no more voters, but the internal structure of these companies would have improved from a democratic point of view.

Anyway, we should not forget that abstentionism in our Western societies has deep roots and does not depend only on the ease of voting (see An99). Simplified voting procedures, like those provided by some e-voting systems, may eliminate some of the reasons for current abstentionism, but obviously not all of them.

Having analysed the arguments in favour of e-voting solutions in countries with consolidated democratic systems, we conclude that, even with trustworthy electoral procedures, new technologies could enrich citizen participation mechanisms.

In any case, not all countries have consolidated systems. Many states make enormous efforts to increase the reliability of their electoral logistics, but are often confronted with corruption, disinterest or with the illiteracy of large segments of the population (II). Can the electronic vote provide positive solutions to this worrying situation? Would we not perhaps be making a mistake by attempting to introduce sophisticated technological mechanisms in countries whose priorities, as we have seen, should be others?

The answer to this question depends not only on the situation with which we are confronted but also on the technological option chosen. Firstly, we should be aware that, although we may find that some countries have structural deficiencies in the socio-electoral area, the differences between them could be so considerable that it is not possible to have a generic approach to questions that require individual study. It should also be said, however, that even in extreme cases the electronic vote can provide positive new aspects.

Brazil and India can serve as a reference given that they are countries where the logistics surrounding elections present very serious problems. Their geographical dimension, corrupt attitudes and the widespread poverty and illiteracy are enormous challenges for any proposal that plans to develop a democratic process. Despite all this, both countries are using electronic ballots.

Brazil, for example, has been able to generalize the use of electronic voting by way of touch screens (see Ri03: § 31-47). The important aspect of this case is that technological modernization has helped to reduce some of the deficiencies mentioned above. In this way, the design of the screen, which emphasized such graphical elements as the photo of the candidate, has allowed both complete and functional illiterate people to exercise their right to vote in a simpler, more intuitive and safer way than the traditional ballot. On the other hand, the fact that computers automatically count all the votes could help to prevent, although not eradicate, the traditional dangers of electoral corruption.

In the case of India**,** elections in 2004 have demonstrated that it is possible to introduce extraordinarily simple electronic systems (see Te04; Id04). Although the model may contain some defects, the novelty of the experience was that it tested a range of electronic voting tools that were not complex but could modernize the Indian electoral process at a reasonable price.

3 Concluding remarks

Having analysed examples from both developing and developed countries, we can conclude that legal electoral regulations cannot be excluded from technological innovations such as electronic voting systems. There are several reasons for this: the need to prevent outdated political systems, the fact that the political participation of specific groups can be improved or the possibility that the current electoral corruption in some countries can be reduced. These innovations should naturally be undertaken with care**.** There is no room for adventurous behaviour, which disregards the virtues of the current systems and hopes to improve these with excessive naivety or technological optimism. It is not admissible, for example, that the electoral fiasco that took place in the United States in the 2000 presidential elections be hastily resolved by way of introducing electronic ballot boxes that had not been adequately controlled (see KSR04). The scandals that have arisen in relation to firms such as *Diebold* do very little in favour of a technological modernization process that, if appropriately implemented, is already an imperative need in current democratic systems.

Neither is it possible to accept those strategies that try to make massive e-voting evaluations without clear rules governing the attendance of independent observers or without officially publishing the results of the survey carried out during the electoral days. Unfortunately, the Spanish Government made these mistakes in 2005 during the referendum on the European Constitution.

4 References

[An99] Anduiza Perea, E.: ¿Individuos o sistemas? Las razones de la abstención en Europa occidental. Centro de Investigaciones Sociológicas, Madrid, 1999.

[AT01] Auer, A.; Trechsel, A. H.: Voter par Internet? Le projet e-voting dans le canton de Genève dans une perspective socio-politique et juridique. Helbing & Lichtenhahn, Bale, 2001. *www.geneve.ch/evoting/doc/voter_par_internet.pdf* [November 30th 2004]

[BR04] Barrat i Esteve, J.; Reniu i Vilamala, J. M.: Informe de las experiencias de voto electrónico empleadas en las elecciones catalanas de noviembre 2003. Universidad de León – OVE / Universitat de Barcelona, León / Barcelona, 2004. *www3.unileon.es/dp/aco/area/jordi/treballs/evot/cat03.pdf* [November 30th 2004]

[BR04a] Barrat i Esteve, J.; Reniu i Vilamala, J. M.: Democracia electrónica y participación ciudadana. Informe sociológico y jurídico de la Consulta ciudadana "MadridParticipa". Ayuntamiento de Madrid, Madrid, 2004. *www3.unileon.es/dp/aco/area/jordi/treballs/evot/llibreesp.pdf* [November 30th 2004]

[Ca03] Calderón Chelius, L. (coord.): Votar en la distancia. La extensión de los derechos políticos a migrantes, experiencias comparadas. (Col. "Contemporánea Sociología"), Instituto Mora, Mexico DF, 2003.

[Ci05] Cisteró i Fortuny, O.: E-Vot vinculant per Internet. Eleccions als càrrecs de la Junta de Govern del Col·legi d'Enginyers Tècnics Industrials de Barcelona. Juny 2005. In: II Jornades de Signatura Electrònica. Agència Catalana de Certificació – CATCert, Barca, 2005. *www.js-e.net/cat/Archivos/ponencies_web/Oriol_Cistero.pdf* [January 5th 2006]

[Fu00] Fundació Jaume Bofill: La votació electrònica: un debat necessari. (Col. "Debats de l'Aula Provença – 33"), Fundació Jaume Bofill, Barcelona, 2000.

[Gr03] Gritzalis, D. A. (ed.): Secure Electronic Voting. Advances in Information Security. Kluwer, Boston, 2003.

[Id04] IDA – Interchange of Data between Administrations: India's massive e-vote considered a success. IDA / European Union – eGovernment News / May 17th 2004. *europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=2551&parent=chapter&preChapterID=0-140-194* [May 21st 2004]

[In03] Informe: Informe de la Comisión especial para el fomento de la transparencia y seguridad en los mercados y en las sociedades cotizadas. Comisión especial para el fomento de la transparencia y la seguridad en los mercados financieros y en las sociedades cotizadas, 8th January 2003. *www.cnmv.es/publicaciones/informefinal.pdf* [November 30th 2004]

[KB04] Kersting, N.; Baldershein, H. (eds.): Electronic Voting and Democracy: a Comparative Analysis. Palgrave Macmillan, Basingtoke, 2004.

[KK05] Kies, R.; Kriesi, H.: Designing internet voting. The potential impact of a pre-voting public sphere on pre-electoral opinion formation. In (Trechsel, A. H.; Mendez, F., Eds.): The European Union and E-voting. Addressing the European Parliament's internet voting challenge. Routledge, London, 2005; pp. 147-165.

[KSR04] Kohno, T.; Stubblefield, A.; Rubin, A. D.; Wallach, D. S.: Analysis of an Electronic Voting System. 2004 IEEE Symposium on Security and Privacy, 2004. *avirubin.com/vote.pdf* [August 18th 2004]

[PK04] Prosser, A.; Krimmer, R.: Electronic Voting in Europe. Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, 2004.

[Re03] Remmert, M.: Developing a common framework for e-voting in Europe: The Council of Europe's draft recommendation on the legal, operational and technical aspects of e-voting. ACEEEO – Association of Central and Eastern European Election Officials, Annual Conference / London – October 2003. *www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting/04%5FBackground%5Fdocuments/07_Presentation_MR.asp#TopOfPage* [August 17th 2004]

[Ri03] Rial, J.: Modernización del proceso electoral: voto electrónico. Observatorio Electoral Latinoamericano, [2003]. *observatorioelectoral.org/biblioteca/?bookID=26* [August 18th 2004]

[Su01] Sunstein, C. R.: Republic.com. Pricenton University Press, Princeton.

[Te04] Techaos: Indian EVM compared with Diebold. Tech Caos, personal blog / May 13rd 2004. *techaos.blogspot.com/2004/05/indian-evm-compared-with-diebold.html* [July 28th 2004]

[TM05] Trechsel, A. H.; Mendez, F. (eds.): The European Union and E-voting. Addresing the European Parliament's internet voting challenge. Routledge, London, 2005.

[Tu05] Tula, M. I. (coord.): Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales. Ariel, Buenos Aires, 2005.

[Va04] Vañó Vañó, M. J.: Transparencia y nuevas tecnologías en las cooperativas de crédito. In: CIRIEC-España, Revista economía pública, social y cooperativa. 49, 2004; p.117-141.

[Va05] Vañó Vañó, M. J.: Derecho de sociedades y comunicaciones electrónicas. In (Plaza Penadé, J., Coord.): Cuestiones actuales de derecho y tecnologías de la información y la comunicación (TICS). Aranzadi, Cizur Menor, 2005; pp. 225-255.

How e-voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals.

Laurence Monnoyer-Smith

Dept. of Human Sciences and Technology
Université de Technologie de Compiègne
BP60319
60203 Compiègne Cedex, France
laurence.monnoyer-smith@wanadoo.fr

Abstract: This paper describes the direct relationship between the perception of citizenship and its material expression, with emphasis on how changing expression obliges a rethink of the channels of mediation between citizens and their elected leaders. An analysis of the French voting ritual will show how our voting system is embedded in a specific cultural conception of citizenship . The emergence of new voting procedures could then be analysed on a social point of view as the will for citizens to rejuvenate some ancient conception of citizenship. I propose a table which maps out the connection between citizenship models and their new technological materialization. A two-way flow of creativity between models and tools which broadens scope for grassroots participation then explains the creation of new rituals as well as the reframing of the role of existing rituals.

1 Introduction

Electronic voting has been gradually establishing itself in the political landscape as voting terminals and online voting replace the traditional ballot boxes of Europe and punchcard machines of the U.S.A [Co02], [KLS04], [No04], [TM05]. Beyond the design issues, voting technology demands new legislation that requires re-examination of the fundamental principles of citizenship and representation developed and applied since the birth of our modern democracies some two centuries ago. While the debate on data security issues and costs has been running since the beginning , the fundamental question of how to adjust existing theoretical models of citizenship to cope with new forms of online democracy has been assessed more recently [CM01], [Ho01], [Sa01], [Co01], [Co05a,b], [Mo03]. As such, the virtual ballot introduces disturbing modifications to the material procedures of the voting ritual [MM02], [OV04], [KLS04]

This paper describes the direct relationship between the perception of citizenship and its material expression, with emphasis on how changing expression forces a rethink of the channels of mediation between citizens and their elected leaders. The availability of new mediation channels need not be seen as the disappearance of a time-honored ritual but as a symptom of change in how voters experience their citizenship. This allows reinstatement of procedures according to a pre-selected model of citizenship that follows

the trend and clearly identifies the risks before technology-based decisions impose restrictions with no public debate. For the purpose of this paper and as an example, I have chosen to describe how new voting technologies challenges the French ritual voting procedure.

2 The Rise of Online Voting

Dreams of better voting systems date back to the early 20th century, largely inspired by rising numbers of voters, multiple elections falling the same day and second-round run-offs that caused many countries to consider replacing ballot boxes with "voting machines"[No04], [Ih93]. However, mechanization was limited to putting some buttons and vote counters in a booth before interest waned fatally after the unpromising results of 1970s trials in Europe and North America.

Only in the late 1980s did the first electronic systems come online, entering use on a national scale in Belgium and Holland in the early 1990s and Brazil in 1996. For its part, France ran a few trials in Bordeaux and Brest in 1980 but the real test of the all-in-one electronic booth with a "built-in ballot box" was the 1999 European Union elections, followed by its use for the 2000 referendum asking citizens whether or not to reduce the presidential term of office from seven to five years. The success of these two experiences led the Interior Ministry to approve three different types of electronic voting systems in its Decree of 18 March 2004.[1] All three are compatible with the traditional voting station but eliminate the need for a ballot box. Without directly threatening the physical survival of traditional voting devices, the systems nonetheless mark a step towards fundamental subversion of the traditional voting process itself[2].

Meanwhile, the Internet started fostering the first political and administrative applications of either technocratic or community-based inspiration in North America and Europe [Ts00]. Most of the first private-sector initiatives were from the U.S.A. where a handful of manufacturers, with a background in onsite/online voting and secure online transaction systems, began to market online voting systems for general meetings of corporate shareholders and of professional associations. In Europe, Germany, Switzerland and the U.K. began studying new voting technologies in the mid-1990s through a series of pilot projects involving television, SMS, postal votes, etc [Mo03]. However, the European Commission (E.C.) soon took the lead in online voting through its Fifth Framework Programme for the User-friendly Information Society [Mo04][3]. By the mid-1990s, the E.C. was a very proactive backer of "digital city" projects, online voting and electronic services, thereby giving Europe a decisive lead in hands-on experience over the U.S.A. where initiatives were more limited.

The issue of remote, online voting differs radically from that of straightforward electronic voting in a polling station because it directly undermines the material basis of

[1] The NEDAP 2.07, RDI-Consortium Univote iVotronic and the Indra Sistemas SA Point & Vote
[2] - For an exhaustive analysis of French experiments in electronic voting systems, see Ledun, 2005.
[3] http://europa.eu.int/comm/research/ist/leaflets/en/whatisthe5th.html.

the electoral process, something the 1975 French ban on voting by mail sought to protect. Thus, one major consequence of online voting is the denaturing of a voting process, even if it has existed in its present form for less than a century [Ih93]. At this point, two attitudes strike me as mistaken. The first is to perceive the new technologies as a threat to a time-honored voting ritual – an opinion widely held among elected officials and researchers in France. The second is to reduce the technologies to a process of mass rationalization of government administration that transforms the citizen into a consumer, thus assimilating the political and economic systems into Niklas Luhman's autopoietic concept of society [Le05]. They are mistaken, I find, because both disregard the social substance of the technological devices. Indeed, voting should be analyzed with all the methodological rigor due to any "total social phenomenon", to quote Marcel Mauss. A full discussion is beyond the scope of this paper but I shall stress the complex interplay of all the dimensions proper to voting (e.g. political, social, economic, technological, legal, communicational) and the need for taking perspective in an area where, more so than elsewhere, the observer is part of the thing observed.

For these reasons, it is pointless to deny that electronic voting undermines a fundamental symbolic construct of our contemporary democracies or that online voting was developed by private enterprise in a bid for a share of e-government markets [KLS04], [OV04]. That said, in light of the above considerations, it is important to note that the introduction of online and other new voting technologies is a symbolically and politically loaded event of a magnitude equal to the introduction of the now-familiar ballot box some 150 years ago.[4] To ignore this is doubtless to misinterpret the call of a part of society that is becoming manifest after the emergence and local appropriation of these new technologies and, doubtless, to remain prisoner of one's own mindset.

3 The Paper Ballot as a Ritualization of Citizenship

The protocol of the voting ritual is a system of constraints, a set of procedures and a symbolic construct that incarnate a set of beliefs. The more this symbolic dimension is anchored in a country political culture, the harder it is to investigate on new voting systems. This explains why, in countries like France, a national pilot program testing alternative voting procedures, such as in the UK or Switzerland for example, could not be envisioned. It is the product of a social convention designed to balance off a conception of the republic, a construct of citizenship and a vision for social order.

As a social phenomenon, it is an original way of materializing the incarnation of a procedure whose gradual ritualization has come to mark the crossover from the secular world to the sacred one. This is quite visible in the French procedure which follows a dramatic narrative structure that elevates to the status of empowered citizen any walk-in to a polling station.

[4] The ballot box was adopted in France in 1848 for mechanical reasons when universal suffrage legislation for all citizens aged 21+ upped the total number of ballots from 250,000 to over 9,000,000. The ballot box then entered a process of gradual symbolization.

Vote casting breaks down into a sequence of physical 'rites of passage' that involve specific positive do's and negative don'ts. It is interesting to read Arnold Van Gennep's diagrams of rites of passage in light of Yves Deloye (2000:10). Van Gennep associates passage from one stage to another with a material dimension that incarnates it as a recurring symbology of birth [Be86]. The voting ritual is a cultural construct that meets a need for higher meaning in a young republic eager to assert its social and political legitimacy, as was France in the 18th century. Borrowing the terms in brackets from anthropology, we can apply this observation to consider the act of voting as a mystical "transition state" [Bo79], which effects transubstantiation of the voter during a "liminal phase".[5] Reinforced by the privacy of the voting booth introduced in 1913, the transition state is all the more necessary insofar as political science theory makes the Nation-State the sole source of all legitimate power instead of citizens as individuals. However, the Nation-State remains an abstract concept far removed from the people, which leaders have learned to mistrust. The voting ritual operates transmutation of the people into the Nation-State by extracting from each voter a sample of that sovereign nationhood. The preliminaries serve as a separation rite that mourn the citizen's present social status and put it to death.[6] They are prerequisite to the aggregation of ballots in the urn, after voters pass through the voting booth. The purpose of the rite is to quantify the political will of the citizenry. Thus it ends with a postliminal phase consisting of a one-for-one count of all the ballots that express the opinions of socially unequal and very dissimilar individuals and add up to the Voice of the Nation-State.

It is now easier to understand how online voting can directly aggresses the traditional republican perception of citizenship in a democracy which intensifies the citizen's moral duty to exercise his rights of citizenship; he owes society his vote in exchange for the freedom and protection it supplies. It operates by "stripping the citizen of all social, religious and cultural attributes" [Sc01:81], which involves measures to guarantee the sincerity of the vote the ritual serves to express.

From this, online voting becomes pure sacrilege because of its concern for the voter's convenience (i.e. voting from home at any hour), for more efficient use of time (by both citizens and the government) and above all, for the faith it shows in the voter's ability to make sincere choices in an environment he deems insecure.

4 The Voter Behind the Virtual Ballot Box

The political habits of French and European citizens today differ noticeably from those that evolved since the first ballot boxes came out. Among them, three are of major importance to the perception of citizenship in a democracy.

---

[5] Victor Tuner (1969) prefers "liminality" (from *limen*: doorstep) to describe the stage suggestive of "limbo". Van Gennep's three stags of rites of passage thus become Preliminary (Separation), Liminal and Post-Liminal (Reincorporation).

[6] Separation rites have strong religious connotations that recall Biblical quotes about access to heaven, e.g. "…how hard it is for them that trust in riches to enter the kingdom of God. It is easier for a camel to go through the eye of a needle, than for a rich man to enter into the kingdom of God." (Mark, 10:24-25).

The first consideration is our relationship to time and space. The relentless pressure on people for ever higher productivity and efficiency comes into conflict with a demand for greater availability that government is hard-pressed to satisfy. Moreover, the greater mobility that technology affords makes it increasingly difficult for some persons to be available, given the requirement for physical presence at the polling station.[7]

Second, the citizen's relationship to the Nation-State has evolved greatly in the past century. Paternalism petered out after the 1968 uprising, as did condescending attitudes toward women. The proliferation of procedures for concerted action and public debate in numerous fields of civil and political activity[8] confirm recognition of the need for more two-way information flow between elected officials and voters as well as between experts and laymen. In line with Tom Janoski, I see the expansion of "active" political rights[9] as a noteworthy trend in modern democracies that perceive citizens as dialogue partners rather than just electors. By raising the French Republic to a sacred symbol of our common will to live together, the voting ritual clashes with recent developments that effectively reduce the symbolic distance between the citizens and their elected representatives.

However the most fundamental issue is what Ulrich Beck and Anthony Giddens call "reflexive modernization", which best explains the undermining of the three stages of the traditional voting ritual. It holds that the individual appropriates his social status as part of his personal identity but without perceiving that status as a determinant of his behaviour or lifestyle. Therefore, the physical isolation orchestrated for the liminal ritual to protect the citizen from indiscreet onlookers may be out of step with the perceived experience of voting. Many voters find that ritual isolation feels unnatural, especially in deliberative situations where individuals are valued for the unique worldviews endowed by their social positions [Yo99][10]. From this standpoint, reflexive modernity explains the trend whereby the individual who is accustomed to the rules of modern democracy becomes an agent for social change and appropriates the determinants bearing down upon him. The condescension and guilting (i.e. the citizen needs protection against himself and might be wanting to influencing others) of the liminal ritual seem out of step with the political practices of today's modern democracies.

The citizen of the digital era no longer fits the image foisted upon him by the traditional voting procedure. From this standpoint, the gradual erosion of the ritual induced by recourse to voting machines and online elections in Switzerland and elsewhere, ties in with a will to redefine citizenship, which needs new forms of materialization and post-modern rituals. It is therefore important to consider as a whole all the technological

---

[7] - In many countries, proxy voting is subject to strict requirements. Applicants must present at the defense ministry police (Gendarmerie), justify their absence on election day and the proxy must be a resident of the same voting district as the applicant, a condition harder to meet in larger urban agglomerations.

[8] - The theory of deliberative democracy which refers to a specific form of participation through discussion has played a determinant role in the development of such procedures. Among a huge academic literature, see Barber, 2003.

[9]- "Political rights refer to the right of participation in the public arena and are largely procedural, but the content of legislation is not usually part of political rights themselves" (1998:30).

[10]- Yves Deloye (1993) thus outlines various personal strategies to avoid the isolation of the voting booth by voters who feel they can make their choice discreetly without it.

constraints and models of citizenship in a debate that includes all players in the public arena. Some scholars have mapped out new definitions of citizenship in a digital era ([Cm01], [Ho99]) and have tried to link them with new ICT tools offered by local or national authorities. These models nevertheless tend to be driven by a deterministic approach to technology: they either associate new categories of citizenship with specific type of e-tools [Cm01], or build up a new citizenship : the digital one [Ho99]. Inspired by Janoski (1998) and Benjamin Barber (2003), I suggest in the table below to link the evolution of the conception of citizenship (from passive to more "active" and participative rights, [Ja98]) with their actual usage in modern democracies. This table suggests relationships to primary type of decision-making involved with a selection of their new materializations[11].

Model	**Administrative**	**Referendum**	**Republican**	**Deliberative**
Citizenship Concept	Systemic: citizens are numbers protected by a legal arsenal	Liberal: citizens are autonomous and wary of government	Republican: citizens are bound by a system of shared values. Strong integration: citizens are deferential towards government	Neo-Social:[12] Various corporate bodies involved in the government decision-making process
Relationship to Decision-Making	Action taken on applications with or without input from ad hoc commission(s)	Action taken after national referendum	Action taken after broad, legally non-binding consultation(s) with citizens	Action taken after due, legally-binding deliberations
Technology	E-government, Internet protocols, up/downloads and secure online payment	E-voting, E-referendums and Fishkin-type polling	Forums, gateway websites, public debates, conferences	Dedicated websites, online debates, etc.

Figure 1: Categories of Citizenship and their actual usage in modern democracies

Of course, these are weberian ideal-type models of citizenship and could not be found in their "pureness" form in modern states. One could nevertheless acknowledge trends in European or Northern American politics toward specific forms of citizenship by concentrating a national public effort on some of these technologies.

In most European countries for example, important public funds have been dedicated to on-line administrative services to the detriment of e-democracy procedures such as on-line consultations or public forums.

[11]- For an earlier version of this table, see [Mo03].
[12]- Janoski terms this "social or expansive democracy" while Barber calls it "strong democracy", see [Ja98].

This reveals the tendency of our political systems to reduce effectively the conception of citizenship to its administrative dimension rather than its participative one, even if the political discourse often underlines the need for more citizen's involvement in politics [Co01], [Co05a].

As such, electronic voting procedures correlate with conflicting perceptions of citizenship ranging from right-wing to neo-left-wing. However, the hybrid procedures for public debate sooner match a communitarian/republican or embryonic deliberative model. Thus, the new materializations offer a range of competing models of citizenship that combine to favour new ways of exploiting existing technologies. This two-way flow of creativity that broadens scope for grassroots participation assumes the creation of new rituals as well as a reframing of the role of existing rituals. The actual scholar discussion about the concept of "direct representation" [Co05b] correspond to this phase of conceptualisation which follows grassroots participative systems locally developed.

5 Conclusion

The introduction of new voting procedures requires a rethink of the relevance of the symbolism of the pre-existing procedures. To reduce consideration to purely technological, ergonomic or political issues will hardly map out the creative trends now witnessed in the ways in which citizens participate in the political decision-making processes, whether we are speaking of online voting or deliberative procedures. I also feel it is as important to maximize the social dimension of the new technologies used in the political process in order to take account of the major changes they impose on the materialization of our practices.

Our political systems and theoretical models are contingent upon the social practices that ritualize, symbolize and give meaning to them. To map out their development, researchers must set aside any norms about the "best system", which would skew observation of change in political practices. Recent field research and observation of new deliberative practices now yields a hypothesis for a trend into a new model of more deliberative citizenship [Ba03], [Co01], [Co05b]. Public confrontation between two opposing models with radically different consequences provides an opportunity to debate openly the role and future of the citizen in a modern democracy. Such debate would attest to the vitality of the social fabric and should not ignore the materialization of the citizen's voice, failing which discussion would focus only on technical issues. If so, we risk suffering the consequences, especially the symbolic ones.

References

[Ba03] Barber, B.: Strong democracy : Participatory Politics for a New Age. Berkeley: University of California Press, 2003 [1984].

[Be86] Belmont, N. : La notion de rite de passage , in Centlivres, P., Hainard, J., Les rites de passage aujourd'hui. Actes du colloque de Neufchâtel, 1981, Lausanne :L'age d'homme, 1986 ; pp. 9-19.

[Bo79] Bon, F. : Qu'est-ce qu'un vote ? , Histoire, n°2, 1986 ; pp.105-121.

[CM01] Chadwick, A., May, C. : Interaction between states and citizens in the age of Internet : 'e-government in the United States, Britain and the European Union, Annual Meeting of the American Political Science association, San Francisco, 2001.
[Co01] Coleman, S. : The transformation of citizenship ?, in Axford, B., Huggins, R. (eds.) New Media and Politics, London: Sage, 2001; pp.109-126.
[Co02] Coleman, S. (ed): Elections in the 21st Century: From Paper Ballot to E-Voting. Report by Commission on Alternative Voting Methods. London: Electoral Reform Society.
[Co05a] Coleman, S.: Direct Representation. Toward a Conversational Democracy. IPPR exchange, 2005.
[Co05b] Coleman, S. : New mediation and direct representation, reconceptualizing representation in the digital age, New Media and Society, Vol.7(2), 2005 ; pp.177-198.
[De93] Deloye, Y. : L'élection au village. Le geste électoral à l'occasion des scrutins cantonaux et régionaux de mars 1992 », Revue Française de Science Politique, Vol.43 n°1, 1993, pp.83-106.
[De98] Deloye, Y. : Rituel et symbolisme électoraux : réflexions sur l'expérience française », in Romanelli (ed.) How did they become voters ? The history of franchise in modern european representation. La Haye, Kluwer Law International, 1998 ; pp.53-76.
[Ho99] Hoff, J. : Towards a theory of Democracy for the information age , Discussion paper for the Democracy Platform UK-Nordic Meeting, 1999 .
[Ih93] Ihl, O: L'urne électorale, Revue Française Science Politique, Vol.43 n°1, 1993; p.30-60.
[Ja98] Janoski, T.: Citizenship and Civil Society, Cambridge University Press, 1998.
[KLS04] Kersting, N., Leenes, R., Svensson, J. : Adopting Electronic Voting. Context Matters" in Kersting, N., Baldersheim H. (eds), Electronic Voting and Democracy. A Comparative Analysis. London: Palgrave Macmillan, 2004.
[Le05] Ledun, M. : La démocratie assistée par ordinateur. Du sujet politique au consommateurs à caractère politique, Paris :Edition Connaissance et Savoirs, 2005.
[MM02] Maigret, E., Monnoyer-Smith, L. : Le vote en ligne : Nouvelles techniques, nouveaux citoyens ? », Réseaux, n°114, 2002.
http://www.utc.fr/costech/v2/pages/ch_publications.php?id=12
[Mo02a] Monnoyer-Smith, L. : Scenario on electronic citizenship. A roadmap for 2010", First EVE International Conference : E-democracy : scenarios for 2001. Paris, 2002.
[Mo02b] Monnoyer-Smith, L. : Review on electronic voting". First EVE International Conference E-democracy : scenarios for 2001, 2002.
[Mo03] Monnoyer-Smith, L. : Les enjeux inexprimés du vote électronique, Sciences de la Société, n°62, 2003 ; pp. 127-146.
[No04] Norris, P. : Electoral Engineering: Voting Rules and Political Behavior. Cambridge, Cambridge University Press, 2004.
[No05] Norris, P. : Internet voting and democratic politics in an age of crisis", in Trechsel A. (ed.) The European Union And E-voting: Addressing The European Parliament's Internet Voting Challenge, London: Routledge, 2005; pp.223-237.
[OV04] Oostveen, A., Van den Besselaar, P. : Internet voting technologies and civic participation, the users perspective. Javnost / The Public Vol. XI , No.1, 2004; pp.61-78.
[Sa01] Sassi, S. : The transformation of the public sphere ?, in B. Axford and R.Huggins (eds) New Media and Politics, London: Sage, 2001, pp.89-108.
[Sc00] Schnapper, D. : Qu'est ce que la citoyenneté ?, Paris : Gallimard, 2000.
[TM05] Trechsel, A., Mendez, F. : The European Union And E-voting. Addressing The European Parliament's Internet Voting Challenge, London: Routledge, 2005.
[Ts00] Tsagarrousianou, R. : Electronic democracy in practice…One , two, three…countless variants, Hermès n°26-27, 2000; pp.233-246.
[Va91] Van Gennep, A. : Les rites de passage, Paris: Editions Picard, 1991 [1909].
[Yo99] Young, I.M. : Difference as a resource for democratic communication", in J. Bohman and W. Rehg (eds) Deliberative democracy, Cambridge: MIT Press, 1999.

Session 3: Legal and Democratic Issues of E-Voting

The electoral legislation of the Basque autonomous community regarding electronic vote*

Rosa Mª Fernández[1], Esther González[2], José Manuel Vera[2]

[1]Departamento de Derecho Constitucional
Universidad Complutense de Madrid
Ciudad Universitaria s/n
28040, Madrid, Spain
ferrosa@der.ucm.es

[2]Departamento de Derecho Constitucional
Universidad Rey Juan Carlos
Paseo de los Artilleros, s/n
28032, Madrid, Spain
{esther.gonzalez | josemanuel.vera}@urjc.es

Abstract: The Basque Autonomous Community constitutes the only Spanish experience of legal electronic vote regulation. The Basque Government decided, by means of a government bill that was voted in its legislative Chamber on June of 1998, to reform its electoral law and insert, as possible option, an electronic vote by means of a magnetic strip card. This Law, which has not been applied yet, presents a series of important changes and of potential modifications in the Basque electoral system and, perhaps, in the Spanish system. At the same time, in the year 2004, a new government Bill of the Basque autonomous Community is presented in which an electronic vote legal regulation is once again presented. The news regarding the previous project are important. Its processing is interrupted by the dissolution of the Chamber and the new Government formation that, still today, has not retaken up this initiative. The electronic vote in "Euskadi" is a regulated normative topic but that has not yet been utilized in an electoral procedure with binding character.

1 Introduction

Norberto Bobbio indicated that the consolidation and the reinforcement of the democracy are indispensable budget for the transformation of society. For this, the consolidation of all institutions that allow maximum participation to the organs that are attributed with the collective power to make decisions in different levels and the maximum control on the correct execution of the decisions taken is indispensable.

* Work developed under project "Conceptos y sistemas de apoyo a la democracia electrónica" (EDEMOCRACIA-CM,S-0505/TIC/0230)

Deciding is somewhat indispensable for history process, for the development of public powers, for the concreteness of ideas, whatever their type and nature are. The Basque's Parliament decided, in 1998, to incorporate in its electoral law of 1990, a Chapter destined to the electronic vote. This legal regulation was produced like a first and onlyone, in the Spanish electoral system. The general context in which it was devised, so much in a cultural, economic, social, and political perspective, as a legal perspective (Spanish Constitution, constitutional law of General electoral State, etc.) means the object of analysis of this work. The burst of what are called New Technologies has supposed, among others many things, the availability of technological instruments at the service of citizens and of the parliament for exercise of their respective rights to vote.

2 Legal regulation of electronic vote in the Basque autonomous region.

2.1 Basque electoral law 15/1998, of 19th of June

On 9th July, 1998 the Law 15/1998 of 19th of June is published in the Basque Country Official Bulletin which reforms the Law 5/1990 of 15th of June regarding the Basque Parliament elections.

Its EXPOSITION OF MOTIVES expresses, in its second section, that any democratic society should guarantee the participation of its citizens in elections, by which it proceeds to the election of its representatives by means of secret, direct, equal, free, and universal vote. The full exercise of the right to vote requires that, next to traditional manners, new procedures be articulated that allow voters to emit the vote on the electoral polling station, of simple and personal form. The objective that the electronic vote pursues is to allow the articulation of a new form of participation of the citizens in the res publica.

1. Elements of the electronic vote.

The article with which Chapter X begins enumerates the elements that are included in the electronic vote system: magnetic card voting with magnetic strip; electronic ballot box; vote screen; voting booth and software or electoral data processing programs.

2. Organs and distribution of competencies regarding electronic vote material.

In first place, reference is made to the central electoral Committee of Basque Autonomous Community has following competences:

1. Approving the operation validity of the electoral software in magnetic support. This supposes that the data processing program should be validly prepared for the opening and closing of the voting, for the reading of the voting cards with its respective magnetic strips, for the control of the number of cards placed in the ballot box, for the final scrutiny of respective polling station and for the final broadcast of electoral results. Also the software validated in each polling station should be approved, this is, that it collects the necessary information relating to the concrete identification of the polling station, just as is indicated in the following number.

2. Devising the personalization of polling station's software.

3. Guaranteeing the availability and delivery of the software to the electoral Committee of Zone and to the polling station.

4. Receiving, once the elections have been finalized, the magnetic backups of the software and to assure their subsequent destruction.

5. Other functions that the law, or the relative dispositions to the software, entrust it. In second place, the law awards the electoral boards of Historic Territory, the competence to approve the validity of the software "specifications" that will be determined by the Basque Government by means of the Royal Decree. The Royal Decree that, at the same time, will set the characteristics of the booths, models, printing conditions, and making and delivery of the electoral documentation (art. 132 bis IV, 1, second paragraph).

In third place, and for the making and distribution of the cards with magnetic strip, of the electoral documentation and of any other necessary element to the electoral boards of Zone, the Government will be exclusively competent through their home office (art. 132 bis IV, 1). It will also be their competence to assure the availability and delivery of the electronic ballot box, the screen to vote and the voting booth, in each one of the respective electoral polling station.

Finally, the law clarifies that for the development of the functions described the aid of the data processing Service of the Basque Parliament will be included, as a support and advice organ, that it will even be able to participate with voice, but without vote, in the meetings of the electoral boards of Historic Territory or of the electoral board of the CAPV (Basque Autonomous County)

With the new electronic vote, the aid that the data processing Service should lend to the electoral organs in the fulfilment and development of its tasks is indispensable.

Therefore, important technical know-how is required. It is enough to remember that the first task attributed to the electoral board of the CAPV is "to approve the validity of the operation of the software (...)"; or the possibility that the art. 132 twice III, 4, establishes "(...) the general representative of each proclaimed candidacy, by itself or by means of an expert representative in data processing named by it, will be able to obtain, with prior character to its final approval, information on the correct operation of the software from the electoral board of the autonomous region (...)"; articles which doubt who now really passes control over the development of the electoral process. The question that arises regarding this would not be what organ is legitimized by the law to do it, but who is truly qualified for it[1].

3. Regarding the right to vote.

The article 132 ter refers to the "material means and operations prior to voting".

The law sets the need that in each polling station there are two ballot boxes: an electronic one and a traditional one to be able to place, in this one, the absentee ballot, that will be carried out by means of envelopes and ballots. Besides a voting booth will be necessary, or in its absence, a space reserved that allows the voter to be isolated. Both, cabin or space should be equipped with a screen for voting.

3.1 Secrecy in the exercise of the right to vote.

The obligatory character offered by law to the material means that the cabin or space reserved for the voter represents is important. The article 132 quater, I, 2 thus confirms it: "(...) the voter should enter the voting booth and introduce the card with voting magnetic strip in the screen (...)". From this it can be deduced that the electronic vote is "obligatorily secret", in its exercise.

On the contrary, the LOREG (Electoral, General and Organic Bil) article 86.2 determines "(...) the voters will approach the polling station one by one, after to have passed, if thus they desired it, by the cabin that will be placed in the same room, in an intermediate place between the entrance and the polling station (...)" and the article 104.2 of the Law of 1990 of Basque Parliament elections expresses in the following words: "The voter will be able to pass, if desired, by the cabin, collect the ballot of the chosen candidacy, introduce it in an envelope and proceed to voting". Both norms also consider the existence of voting booths obligatory, but these will be able to be or not be utilized by the voters in the exercise of their vote. What evidently strikes an important qualitative difference.

---

[1] "Now, it is certain that the establishment of the electronic vote, be it for periodic elections, be it for referendum consultations, strikes an essential problem of control of the process, that passes from the hands of the electoral boards (legal guarantee), of the citizens and of the representatives of the parties (political guarantee), to be protected by the data processing technicians, with serious the risk that the control be transferred, from the democratic environment to the technocratic stronghold. ..", Pau i Vall, *Democracia e Internet*, Yearbook of Parliamentary and Constitutional Right, Regional Assembly of Murcia, Nº 10, 1998

The different regulation of the secret character of the vote in the three legal norms stirs up the debate around its obligatory character or, on the contrary, its optional disposition to the will of the voter.

The Basque law introduces, with the electronic vote, a vote that is obligatorily secret[2] by demand of the procedure (the screen could have been placed out of the cabin or reserved space), what does not seem to be the same thing than out of courtesy of the constitutional mandate (art. 68.1 CE) the one that describes a secret vote without entering subsequent procedures relating to its execution or its put in practice.

The Constituent consecrated a secret vote, a characteristic not available for the legislator, and no too for the voter. Any legal regulation, or instrument contained in it regarding this characteristic of secrecy, (that embodies the nature of the vote in the Spanish State, along with others cited in the art. 68.1 CE), allow or enable its "availability", will be a clear constitutional breach. Can the universal character of the vote be arranged, deciding to restrict this to certain social collectives? Could it be decided perhaps as more convenient, that only an individual of each household voted for all of its members? Could we be able to accept, for example and for determined people, (businessmen, intellectuals, institutional heads ...) the concession of more than one vote? Evidently, for these cases the respective answers should be equally forceful. The universal character of the Vote is not available, its personal character is not available (existing only exceptional suppositions and valued by a legislator, in which the motive of the exception has had to be fully justified), and the constitutional recognition of the equality of the Vote is not available. The German doctrine is pronounced very clearly. Thus Karl-Heinz Seifers indicates in a comment to the federal electoral Law that "condition sine qua non of a free vote, is a secret vote". In turn, Reinhold Zippelius declares that the basic substrate of the secret vote is to guarantee the free vote. Each citizen has to be able to vote, with the safety that nobody is going to see or interfere in what has been voted. He should always voted without pressures nor alien influences, and Martin Morlok explains that the protection of the secret vote neutralizes social potential power and permits decisions or votes independent from forces or social achievements[3].

---

[2] We also can verify this pretension of the legislator to guarantee a secret exercise in the exercise of the electronic vote in the final Annex of definitions. In it is the definition of what is a voting booth: "A reserved precinct in which the voting screen is placed, in order to preserve the privacy of the vote by the voter".

[3] H. Buchstein, *Präsenzwahl, Briefwahl, Onlinewahl und der Grundsatz der geheimen Stimmabgabe,* page 898-899, *Zeitschrift für Parlamentsfragen*, Zparl. 4, Dezember 2000. The principle of secret vote, just as recognized in the constitutional law art. 38 GG, is not somewhat optional, but a legal obligation for all those who desire to take part in an electoral process. Any harm to this principle will be punishable with liberty deprivation of to two years, or with the equivalent pecuniary sanction (*Paragraph* 107c, Which title is: "*Verletzung des Wahlgeheimnisses*", *Strafgesetzbuch 23rd January, 1974,* modified *BGBl 58/200*); Zittel,T., Elektronische Demokratie: ein Demokratietypus der Zukunft, Seitschrift für Parlamentsfragen, Zparl. 4, Dezember 2000.

3.2 Anomalies in the exercise of voting.

Continuing with the development of the procedure, it is also possible that anomalies in its course be produced (art. 132 quater, III, 1 and 2). In that case, the law indicates that "(...) it will require the presence of the responsible person for the maintenance of the electronic vote material appointed to such effect so that, once the situation is analysed, and the opinion of the referred technician is heard, the President decides if the voting can continue, while the problem is rectified or, on the contrary, to interrupt the voting. .."

Once more, the importance of the necessary technical presence that conditions, if not replaces, the decision of the polling station's President is thus manifested[4].

It can also occur that the voting be interrupted and, in that case, the electronic ballot box must be "resumed", later, operations of emptying and extracting the cards with magnetic strip that have been placed in until to that moment should be carried out and that should be registered again in the hands, logically, of the members of the Polling station.

If the failure is not general, but affects only a voter that cannot register their vote in the magnetic card by means of an adequate use of the screen to vote, the law resolves this supposition with two requirements. In first place, the destruction of the voting magnetic card and, in second place, the delivery of another new validated card, to repeat the operation.

4. Counting time and following operations.

When the electronic process enters the counting phase, article 132 quinques, I and II, in first place, it defines what should be understood as a null vote and a blank vote. And, once the voting time has concluded, the President of the polling station reads the results aloud.

The section III, 5 of the article above mentioned categorically prohibits the possibility to communicate the results obtained, on the part of the electoral Polling stations, to the mainframe computer, before having finalized the counting.

The law also obliges, when the counting has finished, the recovery (for their subsequent erasing and possible reuse) of all the cards with magnetic strips, the ones that are found inside the electronic ballot box, as well as the ones that, by diverse motives, are found out of it (132 quinques, V, 2).

---

[4] GRAY BUESO, J.B., "Democracy and Technocracy: regarding the electronic vote", Parliamentary Magazine of the Assembly of Madrid, no. 3rd June 2000, pp. 64 and ss: "Now well, without denying the functional potentialities that new technologies suppose for the speculative and productive processes and for the dimension of the human knowledge, the movement of these sophisticated technologies to the political process of decision making, should be critically received and established with due cautions, with the shame of converting what could be valid instrumental elements, in any case helpful, in the media and conditioning that end up subverting capital principles of the constitutional system of government and the order of values *insito* to every political democracy".

5. Infractions and Sanctions.

Basic aims of the law are: security, transparency, credibility of this new procedure, simplicity, rapidity, modernity and privacy. In this way, the article 132 sexies enumerates diverse infractions regarding the vote, behaviours that, in some way, undermine those objectives:

a) Voluntary physical or mechanical manipulation of technical elements or of the electronic instruments (vgr. of the screen, of the magnetic cards...).
b) Alteration of the software which is used to count at the polling station.
c) Production, distribution, commercialization and unlawful use of magnetic cards.
d) Destruction of cards during the voting or the counting, with the exception of the cases that thus demand it.
e) Replacement of the magnetic card delivered by the President of the polling station, with a different one, that alters the correct operation.
f) To leave the electoral localities with a magnetic card without authorization.
g) The execution of the counting of the polling station in the case of having suspended the voting.

Chapter X concludes with article 132 septies, titled "Last dispositions". Continued an Annex is enclosed where a series of definitions regarding electronic vote are enumerated.

What deficiencies do the current Right of vote of the Spanish citizen present?

a) The "voting booth" model as a means to guarantee the secrecy of the vote.
b) The complexity and high price of a ballot per each candidacy

Currently, the printing price of the "infinite" candidacies is very high. The possibility of a unique ballot would suppose an important reduction of the expense[5]. It is true that the ballot would be able to contain only the name and symbol of the different political parties whose candidacies have been proclaimed and, at most, the first candidate of the list, what without doubt would imply certain changes for the voter that could not know now, by means of the ballot, is who forms part and in what order is each candidacy presented.

c) The problems derived from the elaboration and updating of the Electoral Census, especially of the CERA, Electoral Census of Absent Residents; furthermore, the numerous problems that the vote through correspondence implies.
d) The present availability regarding the secret character of the Right of vote bears an important interference of this right.

[5] For example, the ballots manufactured for the Elections of June (municipal and European) of 1999 cost 5,776,309 Euros, to what the figure of 2,029,583 Euros was added in concept of printing and envelopes. All of this keeping in mind that the mailing of the parties is credited to them as "electoral expenses", http://www.mir.es/derecho/procelec/loreg/6.htm.

2.2 The new government Bill of 2004

a.1) Exposition of motives and general justification of the new government Bill
Several ideas are explaining in the Exposition of motives of this new normative Text. In all a certain change on behalf of the legislator in his general reflections on the so called New Technologies is appreciated, probably derived from the multiple experiences that this Community has carried out in this matter[6].

1. The apparition of certain prudence or distrust regarding the utilization and application of New Technologies.
2. The perception of two languages and different frameworks, with norms of different operation: the technological framework and the framework of values and democratic principles.
3. The need of a "gradual application" of the New Technologies to the operation and development of democracy. The procedure of electronic vote tries a "sweet" application of the new technologies to the electoral processes. The Basque citizens are going to find a form of exercising the right to vote that, maintaining its characteristic elements, allows, nevertheless, the operation and application of the technologies, and at the same time is perceived without effort by the voter.
4. The conviction that New Technologies are an instrument, not a panacea, and as such should be at the service of "democratic principles".
5. The convenience of maintaining the traditional or classic system of envelops and ballots with the system of the electronic vote.

a.2) Description of the new electronic vote system
The new Chapter X of the government Bill of 2004 begins referring to the elements of the new system of electronic vote that are: a) the voting ballot, b) the electronic ballot box, c) the opening control cards and closing of the ballot box and d) the voting ballots verifying machine (art. 132 bis I).

The ballots, that will have certain resemblance to the classical ballots, will be able to be folded and to be closed. In the internal face of the ballot, the denomination, acronyms and symbols of the corresponding candidacy will be printed.

---

[6]The professor E. Arnaldo Alcubilla indicates that absentee ballots are a voting modality that exempts the presenting of the voter to the polling station the day of the elections, whose recognition, which still presents doubts, very poignantly from a point of view of the personality and secrecy of the vote principles, is based on the enlargement and facilitation of the participation of the electorate and, consequently, of the right of the voters with physical or professionals impediments that cannot attend on the day of the elections to vote personally, Arnaldo Alcubilla, E., "Considerations on the Reform of the electoral Law regarding absentee ballot", in *Reflexiones sobre el Régimen Electoral General*, IV Conference of Parliamentary Right, Congress of the Representatives, Madrid 1993, pp. 711 and ss. The Royal Mint, National Factory of Currency and Stamp, carried out in the year 2002 an electronic vote study for the Absent Residents, VERA system (Electronic Vote for Absent Residents) that has never been applied.
[6] Demotek, (2004) The electronic vote in the Basque Region, electoral processes and documentation direction / Home Office Department www.euskadi.net/botoelek/euskadi/antecedentes-c.htm [12th January 2004].

Likewise, the important novelty that such ballots introduce will be the so called "window of recognition" that appears in the external face of the ballot and that permits: "(…) the identification of the candidacy and other electoral options of electronic form and that can be verified by the voter" (art. 132 bis II. 1).

The function that the window of recognition performs is key in the development of the vote. The counting is carried out, in strict sense, through the window of recognition. In it, the individual electoral information of each voter is contained. "The information contained in the window of recognition will be able to be read with total reliability and security by the reader of the electronic ballot box machine. The electronic vote system fully guarantees the liberty of emission of the vote and the secrecy and counting of the vote" (art. 132 bis. IV).

The electoral Committee, that of the autonomous region as well as those of the Historic Territory, continue being responsible for guaranteeing the transparency and objectivity of the voting procedures and counting in the electoral polling station. For this they can include the support and contribution of the data processing Service of the Basque Parliament.

It also takes into consideration, to a certain extent, the voters that vote by mail and thus the law indicates (article 132 bis VII, 7): "The Government will adopt the opportune measures to guarantee that all the voters, included the absentee ballots, have an egalitarian deal that allows them to verify the chosen option in the window of recognition of the ballot".

In turn, regarding the voting exercise, we can identify the following steps to observe for the voter. 1.- Selection by the voter, inside the cabin, of the chosen voting ballot. With relation to this way of proceeding we should underline that, same as text of 1998, the secrecy of the vote is guaranteed, since thus is arranged to stop being an option. 2.- Verification of the ballot in the "verifying machine" that will read the window of recognition. 3.- The final close and fold of the ballot and its transfer to the electoral polling station. 4.- Delivery of the closed ballot to President of the polling station. 5.- Reading by the electronic ballot box of the ballot.

The procedure can continue from two alternative options: a) that the electronic ballot box, after the reading of the ballot, accepts it or b) that the electronic ballot box rejects the ballot, for different motives, after having performed its reading. In the first case, the shutter of the ballot box will be opened automatically and the President will place the ballot in it, increasing automatically the number of votes that figure on the screen. In the second supposition, the President will return the ballot to the voter inviting him to repeat the observed procedure.

If the vote has been registered correctly the Law establishes that the directors and, in its case the Administrators that desire it, will make a numbered list of the name and the surnames of the voters by order in which they have emitted their vote expressing the number with which they figure on the list of the electoral census. Every voter will have the right to examine if their name and surnames have been written correctly on the numbered list of voters that forms the polling station" (art. 132 quáter I. 4. and 5).

The wording that this new text offers is curious for what should be understood as "supposed accreditation" of the voter; this is done after the reading by the ballot box of the ballot, if this procedure can be identified as such[7], and all this it in spite of the great flexibility with which has always been acted in relation to accreditation of the voter. The Jurisprudence thus confirms it in sentences as that of the Supreme Court of Justice of Navarra of Dec. 4th, 1989, relating to the acceptance of a university card as valid id document or the of the Justice Supreme Court of Catalonia of December 4, 1989 decision that accepted, in similar terms, the copy of the National Document of Identity.

Many are questions that stir up regarding this since in no case is it the prior accreditation required before the polling station of the voter with the opportune documents to the effect. The voter votes before its data is verified (articles 85 and 86.3 of the LOREG), what occurs if after having voter voted and having his/her vote been registered by the electronic ballot box as valid, he/she is not found in the list of the electoral census that the members of the polling station have? We can find ourselves with a voter that may decide to cast their right to vote more than once.

Thus, unless the diligence that is presumed of the members of the polling station, has been truly such, and even then, (article 132 quarter II. 4: "If during the procedure of voting, the members of the polling station observe ill faith on the part of the voter at the moment of voting again with new ballots, the President will take the measures that it reckon convenient to impede actions that hinder the normal development of the voting") we can assure a correct development of the process.

---

[7] The Basque Parliament elections Law 5/1990, of 15th of June, article 105, reformed by Law 15/1998, of 19th June, by Law 6/200, of 4th October and by Law 1/2003, of 28 of March, establishes: "1. The right to vote will be accredited through the inscription in the certified copies of the Census lists or by the specific census certification and, in both cases, by the demonstration of the identity of the voter, that National Document of Identity will be carried out by means of Passport or driving Permit in which the photography of the holder appears. 2. The voters will only be able to vote once. The voting will be carried out in the Section and within the polling station that corresponds, with exception of the Administrators that only they will be able to vote on the polling station in which they exercise their functions. **3. The certified copies of the electoral census lists to which section 1 of this article refers to, will exclusively contain the voters of legal age on the date of voting.** 4. Furthermore, those who accredit their right to be recorded in the Census of the Section by means of the exhibition of the corresponding judicial sentence will be able to vote." Likewise, article 86.3 of the LOREG indicates: "Each voter will declare his/her name and surnames to the President. The Directors and Administrators will verify, by examining the electoral census lists or of the contributed certifications, the right to vote of the voter, as well as his/her identity which will be justified according to what is established in the previous article. Immediately, the voter will deliver the closed voting envelope or envelopes from his/her own hand to the President. Subsequently, the president, without hiding them at any moment from the public, will say the name of the voter aloud, and adding "Votes" will place the corresponding envelopes in the ballot box or ballot boxes.
Also curious is the Agreement of the Central electoral board of March 7th, 2000, regarding "the flexibility regarding the identification of the voters of Las Palmas and Tenerife, given that on Saturday 11 of March is the last festive day of the carnival in the Canaries and it is possible that the voters attend the ballot boxes with attires that be not habitual": "Without damage of the application of the legal precepts and interpretive criteria of this Council as for the identification of the voters and of the necessary seriousness of the electoral act, the polling stations should act with the flexibility advised by the circumstance to be March 12th, piñata Sunday, which refers to the attires with which the voters could attend with".

The problem would be produced, in any case, as a consequence that it be prior to the introduction of the ballot, properly manipulated[8], in the electronic ballot box without having to verify the census data on behalf of the members of the polling station, at least thus is how it is read as articulated.Subsequently, the President returns the "faulty" ballot to the voter and he invites the voter to elect a new one and to repeat the process of voting.

Finally, the 2004 text, object of our study, strike in its surprising article 132 quinques I: "1. There is not a ballot with the option of a null vote. 2. The electoral boards of Historic Territory will resolve the validity of the ballots reserved by the polling station in the cases predicted in the articles 132 quáter VII and 132 quinques VI. 3 of the present Law, being able to declare the nullity of the vote in the following supposition: a) When the vote is emitted in different a ballot from the official model. b) When the ballots contain, in its exterior, insults, expressions alien to the vote, signs of recognition or any another type of substantial alteration. c) When the absentee ballot contains more than one ballot per different candidacy. If there it was an envelope of vote by correspondence with more than one ballot of the same candidacy will be computed as a single vote".

Lastly, the article 132 quinques II regarding the blank vote indicates: "1. Blank votes will be those that: a) Are emitted in electronic ballot with the option of blank vote. b) are emitted in electronic ballot of a candidacy legally retreated of the electoral district. 2.- In spite of what is indicated in section 1.b), in the electronic counting of the polling station, the votes casting in favour of a candidacy legally retreated will be computed to such retreated candidacy and of the same form will figure in the Minutes of Session of the polling station. Subsequently, in the general counting, the electoral board of Historic Territory will consider such votes as blank votes.

a.3) The counting

Once the voting is concluded, the text of 2004, strikes two counting possibilities. Or the electronic counting, that is carries out provided that there were no problems and is done through the opportune manipulations of the electronic ballot box (art. 132 quinques IV, V), or what is called electronic-manual counting.

1.- In what circumstances can this type of electronic-manual scrutiny be performed?
This type of counting is only feasible when the polling station decides, by the majority, to accept the protests or claims presented against the result of the electronic counting that has been carried out.

Thus, the President will take note of the turn out and re-count the contained ballots in the ballot box the electronic-manual way. We would be before a closer recount mechanism species to a classical recount, what causes greater doses of civic confidence. The greater simplicity and comprehension on behalf of the voter of any of the operations and of their development, the greater confidence and sensation of security they have.

---

[8] Article 132 *quáter* II. 2 and 3: "If for any reason the voter's ballot is rejected by the electronic machine of the ballot box, the President of the Polling station at that moment will return the faulty ballot to the voter and he will invite him/her to elect a new voting ballot. The President of the Polling station should verify that the closed voting ballot that he receives from the voter does not contain, in its exterior, expressions alien to the vote or signs of recognition, or any other type of substantial alteration. In this case, the President will not admit this ballot and he will invite the voter to vote again".

2.- What does this type of counting consist of?
The article 132 quinques VI, describes it in detail. The recount only will be performed by the verifying machine located in the voting booth and that should be transferred at the polling station. In no case will it be permitted to open the ballots of electronic voting to avoid their possible deterioration and the consequent annulment of votes that have been emitted as valid. The process begins with the opening of the ballot box by the President of the polling station who will carry this out in the presence of the remainder of members. He will extract all the ballots of the electronic ballot box and he will pass them out one by one by the tester apparatus for the sake of a new reading on the screen.

3 Some desirable recommendations[9].

When we speak of new Technologies applied to the right of vote we mix two very different frameworks, with very different languages and characteristics. Now, the electronic vote, a formula that results from exercising the right of vote by means of instruments from such New Technologies or electronic Technologies should arise under a possible sole plan that is the one that our Legal Code designs and permits.

Our right of public participation through the direct, equal, free, universal and secret vote should remain fully guaranteed and only thus will we be able to try to implement an electronic vote destined, at every moment, to improve or to perfect the regulation of our present electoral vote.

1. Any regulation on electronic vote should part from its nature as "instrument" to the service of our Right to Vote.
2. To undertake a replacement of the present system of voting with envelopes and ballots, the advantages and benefits that the new proposed type of voting would contribute should be sufficiently accredited, and be possible in our legal system.
3. Any reform should part from the identification and faithful diagnosis of the present reality. The instrument should be designed from existing deficiencies and needs to try to alleviate them or rectify them.
4. Any reception of a new instrument should be done under the full knowledge[10] of the intended and not intended nature, characteristics and effects from it that could be derived.

---

[9] We furthermore refer to the Recommendations that the Council of Europe has elaborated regarding electronic vote, *Council of Europe* (2004) *Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical standards for e-enabled voting (IP1-S-EE), Integrated Project 1 –Making Democratic Institutions Work, IP1 (2004).*

[10] The full knowledge, inescapably, carries out experimental tests that are capable of offering data for the reflection and analysis. Thus, for example, we know that recently the present Government has approved a new pilot experience, this time of a national scope, of electronic vote, without legal efficacy, for 52 different municipalities, one for each one of the Spanish provinces during the referendum for the voting of the European Constitution on 20th of February. The Home Office will select the localities in function of its representatives and the sample of citizens that are able to emit their vote electronically will revolve around the two million voters, this is, 6% of the census approximately. Observatory-eDemocracia, 10/2005, (www.edemocracia.es)

5. Finally, we should mention that the potential that the New Technologies contain does not turn out to be at all contemptible. Any democracy should be benefited of these new tools, but we do not want to build a giant with clay feet. It is necessary to take the steps in an orderly fashion, with a parallel analysis of price-benefit that at times will advise us not to adopt a determined position or a determined mechanism.

We finish with a reference that professor Aguiar de Luque offers us, which is the future of democracy in an time in which the information and communication technologies redesign the places where politics unfold, borders are broken down, limits of space and time overflow and old type of discourse is annulled creating a new a subjectivity? If this it is the effect of change, it is not only a private model that is in effect, it is the society in its entirety that day by day is being transformed by these named new technologies[11].

References

[Al98] Alcubilla A. y D'Ambrosio i Gomáriz A., El voto electrónico: algunas experiencias recientes, Cuadernos de Derecho Público nº 4, mayo-agosto, 1998.

[As97] Assemblèe Parlementaire du Conseil de l'Europe de 22 de avril de 1997.

[Bu00] Buchstein H., Präsenzwahl, Briefwahl, Onlinewahl und der Grundsatz der Geheimen Stimmabgabe, Zeitschrift für Parlamentsfragen, Zparl. 4, Dezember 2000

[Ca00] Cano Bueso J. B., Democracia y tecnocracia: a propósito del voto electrónico, Revista Parlamentaria de la Asamblea de Madrid, Nº 3, junio 2000.

[Ca99] Carter M., Speaking Up in the internet age: Use and Value of Constituent E-mail and Congressional Web-sites, Democracy, Parliament in the age of the internet, Parliamentary Affairs, v. 52, nº 3, july 1999

[Do00] Doug Brown, Is virtual voting ready for real time?, ZDNet News, January 2000.

[Fi95] Fishkin J., Democracia y deliberación. Nuevas perspectivas para la reforma democrática, Ariel, Barcelona 1995.

[No99] Noam E., Why Information Technology is Bad for democracy, American Associaation for Public Opinion Research, Media studies Center 1999.

[Pa98] Pau i Vall F., Democracia e Internet, Anuario de Derecho Constitucional y Parlamentario, Asamblea Regional de Murcia/Universidad de Murcia, nº 10 1998.

[Pa99] Pau i Vall F. y Sánchez i Pycaniol J., Democracia y nuevas Tecnologías, VI Jornadas de la Asociación española de Letrados de Parlamentos autonómicos, Pamplona 1999.

[Sa99] Sánchez Muñoz O., Sistema electoral y principio de igualdad de sufragio, VI Jornadas de la Asociación española de Letrados de Parlamentos autonómicos, Pamplona 1999.

[Sa97] Sánchez Navarro A. J., Telemática y democracia, en José Asensi Sabater (coord.), Ciudadano e Instituciones en el Constitucionalismo actual, Tirant lo Blanch, Valencia 1997.

[St99] Strassman M., Internet Voting Circa 2002, Intellectual/Capitol.com, May 1999.

[Zi00] Zittel T., Elektronische Demokratie: ein Demokratietypus der Zukunft, Zeitschrift für Parlamentsfragen, Zparl. 4, Dezember 2000

[11] Aguiar de Luque, L. "El impacto de las Nuevas Tecnologías sobre el principio representativo", in II Madrid's Assembly Parliamentary Conference, Parliament and New Technologies, Madrid, October 2001, pp. 27 and ss.

E-Voting in Brazil - The Risks to Democracy

José Rodrigues-Filho, Cynthia J. Alexander, and Luciano C. Batista

Federal University of Paraiba, Paraiba, Brazil and
Acadia University, Nova Scotia, Canada
jrodrigues-filho@uol.com.br
cynthia.alexander@acadiau.ca
luciano@lbatista.com.br

Abstract: Literature has shown that countries with strong democratic traditions, such as the United States and Canada, are not yet using electronic voting systems intensively, due to the concern for and emphasis on security. It has revealed that there is no such thing as an error-free computer system, let alone an electronic voting system, and that existing technology does not offer the conditions necessary for a reliable, accurate and secure electronic voting system. In this context, then, what are the risks of e-voting to democracy? In what ways, if at all, can more fragile, less mature democracies be buttressed with e-voting systems? As a key component of e-democracy, it seems that e-voting technologies are to become more secure and increasingly reliable in the near future and will indeed be adopted in many countries. In what ways, if at all, will the introduction of such systems increase voter confidence in the political system, promote citizen engagement in political life, and nurture the evolution of democracy? If both e-voting and e-democracy are emerging based on popular demand - that is, as a demand-driven alternative to current processes, then there is no doubt that they are likely to enhance and improve the efficiency of traditional democracy. However, if e-voting technology is being introduced based on a supply-driven fashion - the technology exists therefore it should and must be implemented - then the implications for democracy should be considered. Brazil's introduction of e-voting offers a cautionary tale of supply-driven technological implication. The purpose of this paper is to demonstrate how the introduction of e-voting in Brazil is highly risky to democracy due to the lack of emphasis on security and the lack of a socially-informed and socially driven approach to technological innovation. The Brazilian example illustrates the democratic implications of a market-driven approach. The lack of a technology strategy designed to promote and extend democratic principles is not surprising given the closed door, market-based negotiations that led to the adoption of e-voting in Brazil. The promise, and indeed, the imperative of a democratic, voter-centered approach as an alternative for the development of an electronic voting system, is explored in the paper.

1 Introduction

Literature has shown that countries with strong democratic traditions are not yet using electronic voting systems intensively, given citizens' and policy makers' concerns about the security of such systems. To date, commercially available technology requires an infrastructure that poses complex technical challenges for reliability and security. Despite our technological process, e-voting technology does not yet provide a completely "secure e-transaction environment" [XM04]. Some authors claim that e-voting will never be error-free [Mo04] and that it is nice in theory [OB04], but that in practice, the risks are too large.

Given the lack of security of e-voting systems, what are the risks of e-voting to democracy when the systems are introduced? Can more fragile, less mature democracies such as those in Latin America, be reinforced and advanced with the adoption of e-voting systems? Indeed, what are the implications for emerging democracies when e-elections engage millions of poor people, many of whom live well-below the poverty line? What are the implications of this costly 'technological imperative' upon the policy priorities of their governments? The contradictions are apparent: most countries in the developed world have held off adopting e-voting systems given their concerns about security and their knowledge of the implications of insecure systems for democracy.

However, costly technological systems are being imposed on citizens in less developed countries, where questions about voting abnormalities can go far beyond the scandal of hanging or 'dimpled' chads discovered and heatedly contested in the 2000 Presidential Election in the United States. Which criteria or benefits justify a full-scale electronic election, when the costs - budgetary, democratic and other - are so high? What are the implications when a public network project is conceived and implemented in the interests of corporate actors without consideration for the needs and interests of millions of illiterate people unaccustomed to even traditional voting methods, let alone electronic systems? In what ways, if at all, might an e-voting strategy be conceived which serves the democratic vision of citizens in less developed countries? These and many other questions have not been posed, let alone addressed.

In Brazil, investments in information technology and other e-government initiatives, such as e-voting, have been evolving without a definition of an appropriate information and communication technologies (ICTs) strategy; there has been scant public policy analysis and little academic research work that assesses the heavy public sector investments in ICTs. Surprisingly, there has been no public sector or academic evaluation of e-voting in Brazil, even in places in which there are claims of tampering in the voting process. There is a need to initiate the discussion about e-voting in Brazil to determine whether the country should continue its e-voting initiative, given the significant resources that have been allocated to carry out electronic elections, and given that the initiative has been driven by market push rather than by the electoral needs and interests of the citizenry.

The Superior Electoral Court (Tribunal Superior Eleitoral – TSE), known as the Electoral Justice, is responsible for election administration in Brazil; it has unexpectedly and rapidly adopted a technological system that has not yet been sufficiently tested even in the developed world. The controversies over e-voting are under way and e-voting technological failures have been documented. More recently, scientists started to worry about computer voting systems and numerous reports have found them vulnerable to errors and tampering [OB04, Ko03, Ha03, Ko03, Ma03].

Previous research work, using data related to expenditures in information technology, compiled from the Electoral Justice, has recognized that investments in e-voting are higher than those allocated to basic social programs which serve the needs of the poor much more effectively, in policy fields ranging from education to health. Consequently, e-voting in Brazil seems to reinforce the digital divide and undermine democracy [RG06].

Democracy depends on healthy and educated citizenship; if technology can further policy objectives around education, health and well-being, then indeed, the investment in innovation can be defended in a less developed country. However, when a market-driven approach dominates, the adoption of technology for technology's sake, without due consideration and strategic efforts to mitigate the foreseen and unintended side effects of technological adoption, then there is an obligation to question the motivation for such an initiative, to assess the implications of the adoption of technology, and to push for public dialogue about the relevance and appropriateness of the current course of action.

If a socially-driven technology strategy were in place, the infusion of technology into the public sector might well serve the needs of citizens, particularly those living at the political, economic and cultural margins of society. This strategy should be one that harnesses the power of technology to enhance the design and delivery of health care through tele-health services such as those being introduced to meet the needs of Canada's northern indigenous peoples, or to support innovation in education through the development of culturally appropriate e-learning initiatives that would meet the needs of rural and remote communities as has been the case with the evolution of the Alaskan Native Knowledge Network in the past decade. Such examples of technological investments might encourage democratic dividends, and serve as important enablers that allow at-risk individuals and communities to participate effectively as citizens and as productive contributors to the local and national economy.

The purpose of this paper is to demonstrate how the introduction of e-voting in Brazil is highly risky to democracy due to the lack of emphasis on security and the lack of a socially-informed and socially driven approach to technological innovation. Brazil was the first country in the world to conduct the biggest election on the planet using e-voting technologies. In 2002, more than 100 million voters cast their ballots on more than 406,000 touch-screen machines scattered all over the biggest country in South America.

The paper provides insight into the imperative of moving away from the user-centered to a citizen-centered approach for the design and development of an electronic voting system. In this empowering or enabling approach, people are viewed as subjects who seek to deepen democracy and not as objects, users or customers. Within a top-down decision-making approach, the needs of the market dominate the user-centered approach and results in aggravating existing inequalities. In this sense, what we can see now in many discussions held by the information society is the user-centered model as an ideal to consider the needs of the people, when, in reality, this model means the use, and abuse, of the user of the system.

2 E-voting Insecurity in Brazil

Literature has shown that, to date, commercially available technology requires an infrastructure that poses complex technical challenges for reliability and security. In short, e-voting technology does not provide a completely "secure e-transaction environment" [XM04]. It is also claimed that e-voting will never be error-free [Mo04] and that it is nice in theory [OB04], but that in practice, the risks are too large. Consequently, what the literature has shown is that there seems to be an emergent consensus that existing technology does not sufficiently attend the principles of computer security. In this case, software can be modified in such a way that the results of an election can be modified, with it being very difficult to be detected [Fi03].

Despite the rather intense debate on the idea of e-voting, literature has shown that countries with a strong democratic tradition are not yet using electronic voting systems intensively, due to their emphasis on security. We understand that both democracy and voting are processes much more complex than its electronic version and a secure voting system in itself is a basic element of a true democracy. The question here is: Why has Brazil started using e-voting technology so early in the evolution of the technological systems, when the country does not possess the domain of this technology? The answer is quite simple. The e-voting project in Brazil is based on a rather technical and reductionist view that neglects both the social and political aspects of e-voting. The implementation of e-voting, under the state and corporate governance, is a project by the current dominant networks towards the commercialization and depoliticalization of ICT that can jeopardize democracy. A market-driven approach appears apolitical; technology is perceived as a value-neutral system that can readily deliver efficiency gains within the democratic market-place. The e-voting technology deployed in Brazil is a direct recording electronic (DRE) voting system; it has been judged by Brazilian experts as being more vulnerable to tampering than any another voting system. For some electronic voting experts, the Electoral Justice has opened the doors for new and sophisticated fraud, more serious than the traditional kind [Ma00, MJ02].

In the developed world, the concerns about direct record electronic (DRE) voting technology are not different. Many reports in the United States articulate the risks of this technology, corroborating with what Brazilian academics and scientists say [TCM04, Ko03]. In the U.S, the controversies over e-voting are not stifled; e-voting technological failures have been registered all over.

More recently, scientists started to worry about computer voting systems and numerous reports have found them vulnerable to errors and tampering [OB04, Ko03, Ha03, Ma03]. Given the stakes, any facet of e-democracy, from e-policy consultations to e-voting, needs to be well-researched. Premature investments in e-voting systems are financially, and democratically, irresponsible.

3 Market-Driven Approach to E-voting

Appropriate technological approaches lost favor in the 1980s under U.S. President Ronald Reagan's administration. The neo-liberal agenda privileges economic efficiency, an objective that the informatics sector has fed in the past twenty-five years. There has been a heavy predisposition in governments, in the developed and developing world, to ignore the socio-political and cultural implications of ICTs.

Technological determinism seems to have prevailed in the decisions to introduce electronic voting in Brazil. Because of this, the nightmares of the electronic dreams have already started to appear, even without a deep discussion within a social vision of the technology, which would be enough to put electronic voting in its right place. A recent study carried out by the Organization for Economic and Development Cooperation (OECD) confirms that, if governments do not learn how to manage the risks of information technology, the electronic dreams will become global nightmares [OEC01].

There is a need to expand the discussion about e-voting in Brazil in order to see whether the country needs an electronic voting system or not, considering that investments in e-voting are higher than that in basic social programs that could help the poor much more in the areas of education and health [RG06]. If people knew how high the cost of e-voting technology is in Brazil, many of them might consider it an expensive toy belonging to the rich and privileged. E-voting systems require a heavy investment in both infrastructure and services, posing serious opportunity-cost evaluation and prioritization. Brazil is confronted with many pressing domestic demands and competing priorities from healthcare, to water and sewage quality to housing and education needs.

Unfortunately, critical questions revolving around conceptions, implementation, maintenance, affordability, and evaluation of possible consequences of implementing e-voting on values, economy, context and politics were not discussed with the Brazilian academy and society as a whole. Will e-voting empower the ordinary people? Will e-voting enhance the opportunities of the poor and illiterate to vote without coercion? Will e-voting avoid vote selling? Or, if e-voting technology is not discussed with the society, will it strengthen the powers of the elites, the rich, the educated and the corporate actors at the expense of the ordinary people? It has already been mentioned that e-voting in Brazil has contributed to reinforce the digital divide [RG06].

Therefore, in the Brazilian context, e-voting investments are more in the ICT than in social development for the protection of the disadvantaged and underprivileged groups. The investments in e-voting are higher than investments in important social projects like the control and prevention of cancer, teaching hospitals to attend the poor and the program of income and employment generation [RG06]. There is no doubt that the technological capabilities for the adoption of e-voting will exist in the near future. It is known that many good initiatives of e-democracy and e-government are operational in many advanced rich countries. But these are countries that are not only rich and highly industrialized, they also have had a vast experience in democracy and good governance. .

When access to clean water and food are questionable, raising the idea of investing heavily in e-voting systems is laughable not laudable. Electronic voting should not be considered a priority for people lacking food, health care and clean water. Before thinking about e-voting and e-Brazil, the availability of all services in traditional, non-electronic format, should be guaranteed to everyone.

The discourse of e-democracy has to be reframed beyond the dominant and mainstream rhetoric, so that the political aspects of ICTs meet the real needs of the 'democratic deficit', disclosing the true promises of technology. The high costs of an electronic election can reinforce the digital divide in the sense that it does not reduce inequalities in access to technology, especially when access is created by market-driven forces or corporate actors and the vote is compulsory. On the other hand, in an environment in which corruption in the election process is not an abstract thing, e-voting can appear to jeopardize democracy. The praxis of e-voting must encompass the issues of e-equity, justice and social inclusion.

4 Voter-Centered Approach to E-voting

It is extremely difficult to develop advanced computer applications to support complex human tasks. In the rational design approach, which is still predominant, computer designers too often use models and concepts that focus on the artefact without paying attention to the context in which the artefact is used. However, during the last years, the importance of context is emphasized in the design of computer tools, applications and systems – the context of using and the context of designing computer artefacts. Consequently, in the close relationship between design and use, it was possible to bring together various computing-related research disciplines, such as information systems (IS), human-computer interaction (HCI), computer-supported cooperative work (CSCW), and software engineering, as well as those social science disciplines that are also concerned with the theory and practice of the design and use of computer artefacts [KM97].

In this work we point out the limitations of viewing computer systems as a tool, as in the case of some HCI-research, in which the user-tool-task model is used. Although user-centered design is advocated in the Human Computer Interaction (HCI) literature, it is not as widely practiced as its proponents believe is necessary [GK91]. It has been claimed that from its inception, HCI has been closely aligned with the modernist program, whereby technology has been objectified, reduced, and 'black-boxed'. The participatory tradition has emphasized that this perspective is more likely to favour executives' workplace perspectives over those of low-status workers [KM97, GK91, SN93, BEK87].

In order to be useful to software professionals, HCI workers are often called upon to simplify the users' world and world-view - to make the users' complex experiences conform to the language of requirements analysis and software engineering, constructing fixed requirements from the ambiguous, exploratory, diverse, and mutable world of the users. In some views of HCI and requirements analysis, there is a tradition of reducing complex concepts to simple relationships, as the users' world is represented in the software developers' domain [Mu04].

On the other hand, one should consider many factors related to the problem being addressed or solved by the system, because the conditions may be used to move the software professionals closer to the users or to move the users closer to the software professionals ("move whom to whom"), creating a reference language [Mu04]. In this way, the recent studies on usability with regard to e-voting systems should be considered as very relevant [BHN03, La04], considering that this new technology should not be used as it is proposed now. In the case of Brazil, there is a need for this kind of study in order to show how poor or elegant the voting machine is in the eyes of voters.

As the field of HCI moves towards a new paradigm of user-centered (rather than system- or programmer-centered) design, there will be expanded opportunities for social theorists to participate in the development of information systems. By drawing on this new HCI perspective, an attempt is made to use the user concept to the analogous concept of voter or citizen. This will be better elaborated and expanded as a base for the design of an electronic voting system, in which the voter or citizen can be seen as an emancipator or radical political agent.

The process of dialogue - the social construction of meaning – will be more complete and will be better informed if its process encourages all knowledgeable people to participate. People are more likely to participate and contribute if they feel that their interests are being represented, typically through a democratic process. They are more likely to criticize and correct the group's understanding through a democratic process that solicits and values the diverse voices of all interests. In this view, the processes of creation and negotiation require full participation [KM97].

If the voting process is an important component of democracy, the democratic system should call upon the voters to develop the most appropriate voting system. An election is always a fairly disorganized activity, and the voters have to discuss how to organize it better. In addition, it seems that in the near future, the democratic process can be enhanced by reliable and trustworthy electronic voting systems, created and negotiated by the voters. If there is hope for a voter-driven voting system development, any technology-driven or market-driven voting system should be seen with suspicion in a true democracy. This is the case in the traditional ones.

It has been mentioned that one major cause of system failures is the exclusion, from the design process, of people who will be using the system. When users are not involved in the development of systems like e-voting, democracy will be put in jeopardy [OB04]. Therefore, with regard to the development of an electronic voting system we should take a political stance explicitly and not just keep focusing on methods and techniques to allow more participation, as it often the case in the literature.

In this and future work, an attempt is being made to raise political issues with regard to the development of an electronic voting system, trying to develop an understanding of the manifestations of power relations in and through ICT and software, when the citizen is nearly forgotten. The history of e-voting in Brazil and all its power relations embedded in it has not yet been told. Attempts are being made to focus on the humanization of the electronic voting system in Brazil that needs to be developed under a more elaborated socio-political approach.

5 Conclusion

The democratic potential of information and communication technologies has been widely discussed in the literature since the 1970s, and dominated the discourse of policy makers in developed countries in the Eighties and Nineties, particularly with the explosion of the Internet Revolution in the mid-Nineties. The initial public discourse around the Information Highway in Canada and the United States began with national discussions about how to define access, and even, whether to see access to the Internet as a public good or public utility. It did not take long for the market to persuade governments that all that was needed were narrow-based definitions of ‘access’, focused on mere technological access rather than considerations of literacy and other factors. Even in developed countries such as Canada, the digital divide persists, keeping vulnerable communities such as Indigenous Peoples and African Nova Scotians at the margins of the Knowledge Society, and maintaining the historic economic marginalization of communities in remote or periphery regions such as Atlantic Canada or Nunavut.

Technology tends to take the path of least resistance. In developed countries, resistance to e-voting has been consistent. Without a market for e-voting systems in the developed world, corporate actors have turned to developing countries. Just as pharmaceutical companies whose drugs do not pass the Federal Drug Administration's criteria push their products in the developing world, so too have ICT corporations cast their market nets in the Southern hemisphere.

While Diebold, the electronic voting machine maker, is so questioned in the United States, in Brazil it has the largest contract in its history by selling e-voting machines to the Brazilian government. In a press release in January 2000, Procomp Amazonia Indústria Eletrônica, a subsidiary of Diebold, announced: "For Diebold, this is the largest single order in the company's 141-year history" [Di00]. Negotiating behind closed doors, without the need for public dialogue, it is not surprising that a voter-centered approach was not developed as an alternative for the development of an electronic voting system.

If both e-voting and e-democracy are conceived and adopted based on popular demand (demand-driven option), then the efficiency of traditional democratic electoral processes may be enhanced. However, if e-voting technology is introduced as a supply-driven operation, it is imperative to identify and assess the risks to democracy.

It seems that the introduction of e-voting in Brazil has been risky business. Democracy is at stake. Health and social welfare are on the line, subject to cutbacks despite growing needs. Technology has dominated and driven the policy agenda. Technological hubris and market imperatives have driven the evolution of the Digital Society, with important democratic implications. Appropriate technological processes can reverse this trend in a way that ensures that we are not travelling along the path of least resistance.

References

[BHN03] Bederson, B.; Herrnson, P.; Niemi, R.: Electronic Voting Systems Usability Issues, CHI 2003, ACM Conference on Human Factors in Computing Systems, 5(1), 145-152, Florida: Ft. Lauderdale, 2003.

[BEK87] Bjerknes, G.; Ehn, P.; Kyng, M.: Computers and Democracy: A Scandinavian Challenge. Aldershot, UK: Avebury, 1987.

[Di00] Diebold – News Releases, 2000. Available online at http://www.diebold.com/news/newsdisp.asp?id=2636. Accessed on 25/09/2005.

[Fi03] Fischer, E.: Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. Congressional Research Service (CRS) Report for Congress, 2003.

[GK91] Greenbaum, J.; Kyng, M.: Design at Work: Cooperative design of computer systems. Hillsdale, NJ: Erlbaum, 1991.

[Ha03] Harris, B.: Black Box Voting: Vote Tampering in the 21 Century. Elon House/Plan Nine, 2003.

[Ko03] Kohno, T.; Stubbefield, A.; Ruvin, A.; Wallach, D.: Analysis of the Electronic Voting System. John Hopkins Information Security Institute. Technical Report TR-2003-19, July 23rd, 2003.

[Ko03] Konrad, R.: E-voting critics point to security hole. California primary results appeared online before polls closed. Associated Press MSNBC News, 2003. Available online at http://stacks.msnbc.com/news/964736.asp?0dm=n15ot. Accessed on 20/09/2005.

[KM97] Kyng, M.; Mathiassen, L.: Computers and Design in Context. The MIT Press, Massachusetts, 1997.

[La04] Laskowski, S.: Putting People First: The Importance of User-Centered Design and Universal Usability to Voting Systems. National Institute of Standards and Technology, Gaithersburg, MD, 2004. Available online at www7.nationalacademies.org/cstb/project_evoting_wq_sjl.pdf. Accessed on 30/09/2005.

[Ma00] Maneschy, O.: Fraude Eletrônica nas Eleições, 2000. Available online at http://www1.jus.com.br/doutrina/. Accessed on 10/01/2002.

[MJ02] Maneschy, O.; Jacobiskind, M.: Burla Eletrônica. Rio de Janeiro: Fundação Alberto Pasqualini, 2002.

[Ma03] Manjoo, F.: Hacking democracy?, 2003. Available online at http://www.salon.com/tech/feature/2003/02/20/voting_machine_standards. Accessed on 16/09/2005.

[Mo04] Moynihan, D.: Building Secure Elections: E-Voting, Security, and Systems Theory. Public Administration Review 64(5), 2004, pp. 515-528.

[Mu04] Muller, M.: HCI as Translation Work: How Translation Studies can Inform HCI Research and Practice. CHI Workshop on Reflexive HCI, 2004.

[OEC01] OECD: The Hidden Threat to E-Government: Avoiding Large Government IT Failures. PUMA Policy, 2001.

[OB04] Oostveen, A.; van den Besselaar, P.: Ask No Questions and Be Told No Lies. EICAR Conference CD-ROM, Copenhagen, 2004.

[RG06] Rodrigues-Filho, J., Gomes, N.: E-Voting in Brazil – Exacerbating Alienation and the Digital Divide. 6th European Conference on e-Government, Marburg, 2006.

[SN93] Schuler, D.; Namioka, A.: Participatory Design: Principles and Practices. Hillsdale, NJ, USA: Erlbaum, 1993.

[TCM04] The Caltech / MIT Voting Technology Project. Residual Votes Attributable to Technology – An assessment of the Reliability of Existing Voting Equipment, 2001. Available online at www.vote.caltech.edu/Reports/index.html. Accessed on 10.02.2004.

[XM04] Xenakis, A.; Macintosh, A.: Procedural Security in Electronic Voting. Proceedings of the 37th Hawai International Conference on Systems Sciences, 2004, pp.118a.

Session 4:
Analyzing Solutions for the Uncontrolled Environment

Multiple Casts in Online Voting: Analyzing Chances

Melanie Volkamer[1], Rüdiger Grimm[2]

[1]German Research Center for Artificial Intelligence (DFKI GmbH)
Stuhlsatzenhausweg 3
66123 Saarbrücken, Germany
volkamer@dfki.de

[2]Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz, Germany
grimm@uni-koblenz.de

Abstract: We analyze multiple casts as an easy and non-technical approach to overcome some of the open questions and risks of online voting. The mechanism of multiple casts can be added to almost all existing online voting systems. Nevertheless, there are also some disadvantages, for instance the validity of a timestamp, which are discussed in the paper as well.

1 Introduction

Multiple casts in online voting became popular by the Estonian's legal binding Local Government Council Election in autumn 2005. The voters had the possibility to cast several electronic ballots from different places and devices before the election day. Only the last one was counted. In addition, the voter could cast a paper ballot in the polling station on the election day. In case a voter cast a paper ballot, this paper ballot was counted and any of his electronic ballots was deleted. The Estonian government applied multiple casts in online voting to overcome the discussion about remote voting like voter coercion and ballot buying, because in Estonia postal voting is currently only allowed for citizens living abroad.

The Estonian approach caused a controversial discussion in the (e-)voting community. Nevertheless, multiple casts in online voting is not a new approach, it is not even specific for online voting. Multiple casts in voting are already applied in some countries, e.g. in most of the Scandinavian countries, in the traditional voting system to limit the risks of remote voting in general and to overcome the problem that remote voters are early voters and could not response to short-term political events otherwise. Other reasons are the transmission time and the missing receipt within postal voting. For

instance, in Sweden the voters have the possibility to cast their vote in the polling station even if they already applied remote voting (postal voting or voting in a post office). The ballot cast in the polling station is counted and the remote ballot is deleted. The disadvantage of the Swedish approach is the long period to count the postal ballots because the electoral staffs have first to verify whether the voter cast a ballot in the polling station. With paper ballots, this check cannot be done automatically but it would be possible within online voting.

Thus, some countries have already recognized the advantages of multiple casts in voting. Why do we not utilize these advantages for online voting in general? Is it possible? Are there any other advantages or disadvantages? Does it overcome existing problems and open questions of online voting? To get an answer to all these questions we analyze multiple casts in online voting. We start with an introduction of security requirements and threats to an online voting system in section 2 and identify the open problems specific for online voting in section 3. In section 4 we present different forms of multiple casts in online voting. The advantages will be discussed in section 5 and the disadvantages in section 6. Besides the disadvantages, we will explain in section 7 those mechanisms and techniques, which are necessary to apply multiple casts in online voting. In addition, we will analyze the application with the existing voting systems and approaches in section 8. Finally, we will conclude with a summery and a recommendation for the application of multiple casts in online voting.

2 Requirements and Threats of Online Voting Systems

The main principles of election laws are similar in all democracies. Democratic elections have to be at least *universal, equal, free* and *secret*. Starting from these basic principles, many researchers deduced technical requirements for an online voting system and organisational requirements for the application of online voting. The most popular system and protocol independent requirement catalogues are the Recommendations of the Council of Europe [CoE04] and the Catalogue of Requirements for "Online Voting Systems for Nonparliamentary Elections" of the Physikalisch-Technische Bundesanstalt [PTB04]. These are the main technical requirements to an online voting system:

Deduced from the *universal* principle the election system must ensure that no eligible voter is excluded from the election - $\mathbf{Req_u}$. This must also hold for any kind of server or client software breakdown as well as communication breakdown. In addition, no voter has the possibility to cast more than one ballot within such a break down (equal). To ensure the *equality* principle, no unauthorized person should be able to add, remove or alter votes undetected. This must hold during ballot casting - $\mathbf{Req_{e1}}$, ballot transmission - $\mathbf{Req_{e2}}$ and ballot storage - $\mathbf{Req_{e3}}$. The principle of *secret* elections demands that only the voter is aware of her voting decision. Nobody else is able to link the voter to her vote neither during nor after the election - $\mathbf{Req_{s1}}$. In addition, voters must be unable to prove their voting decisions - $\mathbf{Req_{s2}}$. There are two more requirements, which are less technical but more general. The principle of free elections requires that voters cast their ballot free of duress and without influence - $\mathbf{Req_f}$. In addition, the principle of equal elections requires that all voters can cast their ballots in the same way - $\mathbf{Req_{e4}}$.

An attacker has four attacking points either in order to *break the ballot secrecy* (violation of the secret and free election principle) or to *manipulate the election result* (violation of the equal, free and universal election principle):

Observing a voter casting her ballot - The attacker could be next to the voter casting her ballot in order to observe the voters choice or to coerce her to vote in a specific way (e.g. imaginable in an old people's home) - $\mathbf{Threat_O}$. This is not an online voting specific attack but one for any remote voting system because the electoral office cannot ensure that voters cast their ballots in a free and secret environment. This is why postal voting is not allowed in many countries, and in some countries only as an exception.

Manipulation of the voters' voting device - The attacker could also program malicious code and try to install it on the voter's PC. This code could read the voter's ID, and vote on his behalf - $\mathbf{Threat_{D1}}$, or change the voter's choice before sending it to the electoral server - $\mathbf{Threat_{D2}}$. Moreover, attacking the voter's PC is much more critical than the observation attack from above because now it is possible to manipulate or read several votes automatically. Of course, this attacker needed technical expertise.

Manipulation or sniffing on the communication layer - The Internet is a public network so we cannot prevent an attacker to read or manipulate the connection between the voter and the electoral servers. The attacker can try to manipulate the election result by changing, adding or deleting ballot messages on the network - $\mathbf{Threat_M}$. He can also read and store messages in order to evaluate them - $\mathbf{Threat_S}$. The attacker could wait until someone will find a fast algorithm or faster PCs to decrypt the stored messages.

Manipulation of the election servers - The election servers store beside other data both information, the voters' IDs and their votes. Thus, an attacker could try to get access to the election servers in order to get the corresponding data - $\mathbf{Threat_{E1}}$. He could also try to manipulate the servers - $\mathbf{Threat_{E2}}$.

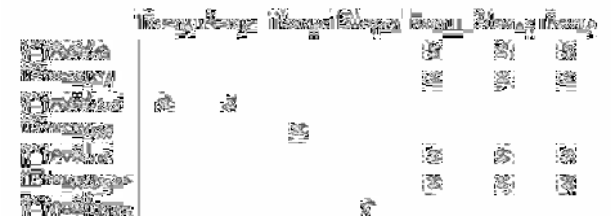


Figure 1: Comparison Requirements - Threats

The table in Figure 1 illustrates which threat violates which security requirement.

3 Open Problems

Many different approaches exist to overcome the threats above and to meet the identified requirements. For an overview over different approaches, see e.g. [Lip05, Sch00]. Most requirements are fulfilled by the existing online voting systems but some unsolved

problems exist nevertheless. Some open problems can be identified by **deduction from the identified threats**. Others stem from **functional requirements**, and from **voting in advance**. These are discussed in the following.

Problems deduced from the identified threats: Obviously, a remote online voting system does not overcome the observation problem - $\mathbf{Threat_O}$. As long as there is no technical or organizational approach to overcome this basic problem remote online voting will only be applied in parallel to postal voting - at least for important elections like parliamentary ones. The main technical challenge, which has not been solved yet, is the malicious code on the voter's PC - $\mathbf{Threat_{D1}}$, $\mathbf{Threat_{D2}}$. There are some approaches like the assistance guidelines for the voters within the elections of the Gesellschaft für Informatik [Gi05], and the theoretical approach of Fischer and Zuser [FiZu05] where the voter does not enter the original vote but a scrambled one. The disadvantages of the existing approaches are organizational assumptions and usability. Thus, a convincing solution to this problem is still missing. Another unsolved problem is the temporary unlimited election secrecy against attackers sniffing on the internet - $\mathbf{Threat_S}$. In [VoKr06] the authors illustrate that the election secrecy is only ensured under corresponding cryptographic assumptions. However, if someone finds a fast algorithm or if he has enough computational power he will be able to link each voter to her vote. The only possibility known so far to enforce theoretical information security with respect to the election secrecy and with respect to attacker sniffing on the Internet is the application of a One-Time-Pad. However, this implies a very high organizational investment.

Other open problems: One main problem in the context of online voting is to ensure that the voter can cast one and only one vote even when her local system, the communication system or the servers break down at any arbitrary step. This is a very important **functional requirement** in the context of online voting. It is hard to ensure this requirement because arbitrary things can happen, e.g. programming errors or an interruption of power supply or communication breakdowns. Another problem with respect to remote and especially postal voting is the **voting in advance**. In traditional postal voting without multiple casts, once the voter has cast her ballot, she cannot change her mind again for any reason, even if political events would cause her to do so. With online voting it is less a problem than within postal voting because the transmission time is much shorter. However, online voting would have problems to guarantee availability if everyone would cast the e-ballot on the Election Day, especially in the last few minutes before closing the election.

4 Forms of Multiple Casts in Online Voting

There are several possibilities to apply multiple casts in online voting which look similar on the first view. But from the organizational point of view they use different methods to ensure that multiple casts are counted only once even if voters use different channels: online voting, postal voting, and traditional voting in the polling station.

(a) The easiest form is to allow online voting exclusively, whereby voters can cast as many e-ballots as they want. *(b)*Within the second form, voters have to decide before the

election whether they want to use online voting or not. Here, a voter receives either a postal voting ballot or the electronic authentication tokens to access the online voting system. Thus, two different electoral registers exists: one for the traditional paper ballot voters and one for the e-voters. The e-voters can cast as many e-votes as they want and only the last one is counted. By doing so, it can be ensured easily that either an e-ballot or a paper ballot is counted.

(c) In the third variant, voters have the possibility to decide during the election time whether they want to apply online voting or not. After having cast an e-ballot the voter cannot cast a paper ballot anymore. But, she can cast as many e-ballots as she wants and the last one is counted. The possibility to apply online voting stops before the Election Day. An election register is printed for the Election Day, which lists all voters who did not cast an e-ballot. Listed voters are excluded from paper voting in the polling station. In addition, depending on the priority, either the e-ballot or the postal ballot has to be deleted to ensure that only one ballot per voter is counted. *(d)* Another possible form of multiple casts in online voting is an extension of (c). We allow voters to cast e-ballots also on the Election Day as long as they have not cast a paper ballot in the polling station. In this case, there is only one electoral register and we have to find a way to delete the e-ballots and/or the postal ballot. A more complicated form would be the following variant (d'): The voter can cast as many e-ballots as she wants, especially also on the Election Day and even *after* having cast a paper ballot. Here, the most favourite form of ballot casting (paper or e-ballot) has to be set up before the election, either uniformly for all voters, or even individually for every voter. For the calculation of the result, it must be possible to remove either the e-ballot or the paper ballot if someone cast ballots using both channels. In all cases it is important to delete the ballots without breaking or endangering the anonymity. Figure 2 illustrates the state machine of the described possibilities.

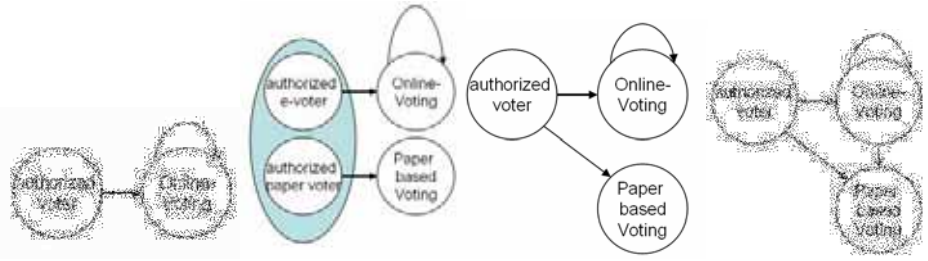


Figure 2: Forms of multiple casts in online voting

5 Advantages of Multiple Casts in Online Voting

Multiple casts in online voting provide a technical approach to overcome some of the open question especially the basic problems with respect to remote voting. The following advantages hold for all forms of multiple casts in online voting described above. First of all the principle of a free and secret ballot casting can be ensured also in the private sector - $\mathbf{Threat_O}$. Of course, an attacker can still observe and force the voter

to cast a ballot but the voter has the possibility to cast later on another ballot and to make another choice. So, it gets unattractive for an attacker to visit people in order to force them to cast a ballot. This is also true in old people's home because the attacker does not know whether someone else will go later on to the same old people's home and manipulate the voters to make another choice. Moreover, any voter who would like to change an unwanted vote could do so at any time. For the same reason, ballot buying gets unattractive[1].

Multiple casts in online voting can also be seen as an easy mechanism to ensure temporary unlimited election secrecy against an attacker sniffing on the Internet and trying to link identified voters to their votes after the election - $\mathbf{Threat_S}$. Strictly speaking, sniffing on the Internet becomes pointless for an attacker because in general he cannot know whether the last and counted ballot of a specific voter is in his memory of sniffed messages or not. The voter could have sent another ballot from another device and thereby over another path - a path on which the attacker is not sniffing. The sniffed encrypted ballots sent over the network become even less meaningful if the voting system allows an e-voter to substitute her e-ballot by a paper one - ***form (d)***. In the multiple casts form (d) an attacker can neither use the sniffed messages to break the election secrecy nor prove to someone else that the sniffed ballots represent valid votes of identified voters. Thus, the application of multiple casts in online voting makes the effort of sniffing and breaking encrypted ballots useless because attackers only get the counted ballots with a certain degree of (unknown) probability. Moreover they cannot use their knowledge to proof it to others.

Another advantage refers to manipulation attacks. When a voter would find out that she has malicious code on her PC during the election time, she is allowed to cast another ballot from an arbitrary PC or from special secure voting terminals or even on paper – $\mathbf{Threat_{D1}}$, $\mathbf{Threat_{D2}}$. With multiple cast, manipulation attacks are only meaning full with respect to result manipulation. The information from the malicious code cannot be used to break the election secrecy because the voter could cast later on another ballot from another device.

There exist two more advantages of multiple cast in online voting. First, the **mal functionality problem** with respect to system or communication breakdowns can be mitigated. If a voter does not receive a receipt at the end of the voting protocol because some problems arose, there is no reason to worry, because the voter can restart the PC, the software and/or the communication and cast her ballot again to get the receipt and to be sure that the ballot is counted. Second, multiple casts in online voting would also overcome the **voting in advanced problem**. A voter can change her ballot at any time at least until the Election Day if some political events happen or the voter has other reasons to change her mind.

[1] This is only true, it the system does not have a receipt mechanism with a zero-knowledge proof. The proof would change for a resubmitted vote and thus the coercer or vote-buyer would notice the resubmission. This does also hold for the temporary unlimited election secrecy in the next paragraph.

6 Disadvantages of Multiple Casts in Online Voting

This new type of voting system with multiple casts does not only have advantages but also some disadvantages. The disadvantages are not specific for online voting in general but for multiple casts in online voting. The main issue of concern refers to the requirement $\mathbf{Req_{e4}}$ that all voters must have the same chances to cast the ballot. *Form (a)* of multiple casts in online voting fulfils this requirement because only online voting is allowed. However, this form can only be applied if every voter has the possibility to cast a ballot (otherwise the universal election principle would be violated). The other proposed forms of multiple casts in online voting - *(b)-(d)* - do not comply with requirement $\mathbf{Req_{e4}}$. Here, the e-voters have the possibility to cast several votes and change their decision while people who are not able or do not have a PC and thus must apply the paper-based election, have only the possibility to cast one ballot. This is especially problematic with respect to the postal voters because they have to cast their vote some days in advance. Moreover, e-voters can get a receipt about the storage of their vote in the electronic ballot box but postal voters do not receive such a receipt. They are discriminated compared to the e-voters with respect to the equality principle.

Currently, at the end of the election most of the systems provide a consistency check. They compare the number of announced voters in the electronic voters register who finished their voting process with the number of votes stored in the ballot box server. This check helps to increase the trust in the system. With multiple casts in online voting, this check is much less meaningful. The voter could announce the vote several times to the electronic electoral register, which would label the voter after the first completed voting process. So, we do not get any statement about the multiple votes cast later on. This unveils another disadvantage of all forms of multiple casts in online voting: It is difficult to verify whether the one vote which is counted is indeed the vote the voter wants to be counted.

Some more disadvantages refer to social aspects: with multiple casts in online voting, we run the risk to loose the seriousness and the value of elections. It becomes similar to a game or some silly polls in the Internet or on TV. Closely related to this is the problem that some critical or unconfident voters could be unsettled which of their votes is actually counted. In addition, with multiple casts in online voting there might arise confusion with election forecasts. While in practise election forecasts are an important part of the election, they must be clearly separated from them.

7 Additional Mechanisms and Techniques

The existing systems have to be extended in order to apply multiple casts in online voting. Several auxiliary mechanisms are necessary and some new techniques have to be developed or have to be taken over from other applications. For example, it has to be ensured that the last cast ballot is the one that is stored and not e.g. the last ballot received at the ballot box. A challenging problem is the deletion of obsolescent ballots. The related function must either delete the e-ballots or destroy the paper ballots in order to allow multiple channel voting as described as ***forms (b), (c)*** and ***(d)***. Another important mechanism is the *timestamp* mechanism for the ballot messages. This becomes

necessary because multiple casts open the door to a new form of replay attacks. An attacker could send an older ballot again in order to manipulate the result. Reliable timestamps can only be provided by a trusted timeserver. The clock of the voter's PC would not suffice, because it is easy to manipulate it. Using the incoming time of a ballot at the ballot box server does not work either, because the ballot message could be withheld by an attacker and forwarded later. Thus, we need a possibility to uniquely assign a ballot message to the time when it was really cast by the voter.

The possibility to cast multiple ballots has to be integrated in the online voting system. There are two possibilities to implement this function. Either the voter's right to vote is checked in the electoral register each time she wants to cast a ballot or it is only verified the first time. In the latter case, the voter would receive an anonymous authentication token, which she uses each time she wants to cast a ballot during the election. Here, the voter needs to have a secure portable memory to store this token. Otherwise, she does not have the possibility to cast the ballot from arbitrary PCs. This could be a smart card, for instance. The problem is that the voter is excluded from casting ballots if this memory gets lost, stolen, or broken. In addition, high security requirements like integrity and confidentiality have to be ensured by the chosen memory otherwise the token could be read out. Therefore, the cheaper, easier and more user-friendly way is the first form: to run through the whole voting process each time again. This mechanism has to be implemented in all proposed forms of multiple casts in online voting.

In some forms of multiple casts in online voting, we have to integrate an additional and very critical mechanism. In ***forms (c)*** and ***(d)*** where the voter can cast both e-ballots and paper ballots the functionality to remove either the paper ballots or the e-ballots has to be implemented. There must be a link either between the e-ballot and the voter or between the paper ballot and the voter, or the voter must be able to remove one of them. This link must be possible without the violation of the secrecy principle (unlinkability forever). At least for the paper ballot election in the polling station the introduction of a link between voter and ballot would downgrade the anonymity compared to the traditional elections in the polling station. In particular for the e-ballots a technical solution must exist which does not violate the election secrecy. There must be a technical means to find the old e-ballot of the voter in the electronic ballot box in order to delete it and to store the new one. A possible solution is provided in [VoRV06].

In addition, the algorithm to replace the old ballot of a specific voter in the electronic ballot box by a new one must be fast. If the algorithm is too slow, the voter has to wait undue until she receives a receipt. ***form (d)*** of multiple casts in online voting requires two additional mechanisms: After the voter cast a paper ballot, the e-ballot has to be deleted and it must be ensured that the voter cannot cast an authorized e-ballot later on. Another mechanism should be implemented in each multiple cast form for online voting: *the wilful abstention from voting after having cast e-ballots*. This means: a voter who has already cast an e-ballot should be able to decide explicitly not to vote at all and thus her already cast ballot to be deleted and not counted. Thereby two things must be done: The ballot has to be secured in the ballot box and a corresponding flag in the voters' register has to be set.

8 Realization of Multiple Cast in Online Voting

There are three types of online voting approaches to overcome the anonymity problem: (1) preliminary voter authentication with subsequent anonymous tokens or pseudonyms, (2) blind signatures and (3) homomorphic encryption. In this chapter, we have a closer look whether multiple casts in online voting can be applied to all of these approaches and which are the respective protocol extensions or new assumptions.

Preliminary voter authentication means, that first the voter sends a request with personal data to the electoral register. This register generates an anonymous token and sends it back to the voter. Second, the voter sends her ballot together with the token to the electronic ballot box. The authentication of the cast ballot is checked by the eligibility of the token. Here it is quite easy to apply multiple casts in online voting because the electoral register just sends the same random token to the voter when she wants to announce a new vote. The ballot box can identify all ballots from one voter by the anonymous token. The difference to the implementation now is that the tokens cannot be deleted after having completed one voting procedure because they are needed for the multiple votes as well. Thus, the anonymity is more endangered and thus the servers have to be better protected. Another variant of preliminary voter authentication is pseudonymous voting. Here the application of multiple casts would be easier with less danger for the anonymity. But, generally, pseudonyms are harder to administrate.

Voting protocols with blind signature are based on Chaum's blind signature algorithm. Blind signatures allow to sign a vote or other data without revealing the content. There are two possibilities to apply this technology to voting protocols: firstly, the voters register blinds the ballot; alternatively, the voters register signs a blinded random token chosen by the voter. The latter one works perfectly with multiple casts in online voting. The random token is sent together with the ballot. Thus, the token can be used to identify all votes from one voter. The first approach to let the voters register blindly sign ballots does also work: currently the voter receives blinded ballots from the voters register for all possible choices. At present, the voter can only choose one of it and send it to the ballot box. With the same mechanism the ballot box now verifies that the voter only sends one of the signed ballots, the ballot box can identify the old ballot of a voter to remove this with the new one in multiple casts in online voting. Here, the application of multiple casts in online voting provides the same anonymity as online voting without multiple casts.

Voting protocols based on homomorphic encryption can also be extended quite easily because the link between an encrypted ballot and the voter is given and can even be proved. Thus, it is easy to replace an old ballot by a new one on the so-called bulletin board.

9 Conclusion

We have illustrated these open problems of online voting: observation within remote voting, manipulation of the voter's PC, the temporary unlimited election secrecy against sniffing on the network, the mal functionality with respect to system and communication breakdowns, and the voting in advance problems. Multiple casts in online voting overcomes some of these problems, namely obviously the remote problem, the voting in advance and the mal functionality problem. The manipulation of the PC is still a possibility for the attacker to manipulate the election result but not to break the election secrecy.

Beyond technology and organizational issues, we should also consider the voters themselves. Security increases only if the voters take the opportunity to cast several votes. Indeed, most of the voters will not do so. In Estonia, they counted 364 of 9681 repeated e-ballots and 30 of them cancelled e-ballots by casting a paper ballot on the Election Day. Therefore, it might be a nice, technically easy but only theoretical solution, which does not overcome the problems in practice. We should also take into account that changing electoral laws in order to allow online voting is not easy in general but it will be harder to allow multiple casts in online voting because multiple casts in voting is not in use in most of the countries. Moreover, there are also disadvantages like the integration of a trusted timeserver, the violation of the equal election with some forms of multiple casts in online voting, and the new mechanisms, which might be critical with respect to the election secrecy. We have identified some open research questions in this context, which have to be solved first.

References

[CoE04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation rec(2004)11 adopted by the committee of ministers of the council of europe and explanatory memorandum. Council of Europe, Straburg, 2004.

[FiZu05] Gerald Fischer and Wolfgang Zuser. The Vote Scrambling Algorithm. Schweighofer E., Augeneder, S., Liebwald, D., Menzel, T. - Boorbergverlag, 2005.

[Gi05] GI Gesellschaft f¨ur Informatik e.V. Election 2005 Assistance guidlines. http://www.gi-ev.de/wahlen2005/ retrieved on 15-2-2006, 2005.

[Lip05] Helger Lipmaa. Electronic voting. http://www.cs.ut.ee/ lipmaa/crypto/link/protocols/ voting.php retrieved on 15-2-2005.

[PTB04] Physikalisch-Technische Bundesanstalt Braunscheig PTB and Berlin. Online Voting Systems for Nonparliamentary Elections - Catalogue of Requirements. http://www. berlin.ptb.de/8/85/LB8 5 2004 1AnfKat.pdf retrieved on 15-2-2005, 8.5.2004.

[Sch00] Schlifni M. Electronic Voting Systems and Electronic Democracy: Participatory E-politics for a New Wave of Democrac. Dissertation Technische Universität Wien, 2000.

[VoKr06] Melanie Volkamer and Robert Krimmer. Secrecy forever? analysis of anonymity in internet-based voting protocols. In (not yet publish conference in April 2006), editor, The First International Conference on Availability, Reliability and Security; The International Dependability Conference Bridging Theory and Practice, 2006.

[VoRV05] Melanie Volkamer, Walter Reinhard, and Roland Vogt. Fuse - ein Internetwahlsystem für zeitlich unbegrenzte geheime Betriebsratswahlen. Sicherheit 2006 ”Sicherheit - Schutz und Zuverlässigkeit”, 22 February 2006.

How to create trust in electronic voting over an untrusted platform

Gerhard Skagestein[1], Are Vegard Haug[2], Einar Nødtvedt[3], Judith Rossebø[4]

[1]University of Oslo, Dept. of Informatics
Box 1080 Blindern, N-0316 Oslo, Norway
gerhard@ifi.uio.no

[2]University of Oslo, Dept. of Political Science
Box 1097 Blindern, N-0317 Oslo, Norway
a.v.haug@stv.uio.no

[3]Senit rådgivning AS
Skogtunet 12, N-1369 Stabekk, Norway
einar@senit.no

[4]Norwegian University of Science and Technology, Dept. of Telematics,
and Telenor R&D
Snarøyveien 30, N-1331 Fornebu, Norway
Judith.Rossebo@telenor.com

Abstract: Casting electronic votes via an inherently unreliable channel like the Internet in an uncontrolled environment is controversial for two main reasons: The first one is of democratic nature and the second of technical nature. The democratic concerns are about the possible dangers of buying and selling votes and so called "family voting". The technical concerns are how to convince everybody involved that the votes will be anonymously and accurately recorded and counted, and that no votes will get changed or lost, and that no "fake votes" will be introduced, with the knowledge that any computerized system may contain bugs or may be hacked by evildoers.

In this paper, we will show how the principle of repeated vote casting may be used to alleviate both the democratic and the technical concerns above, and how hybrid cryptography makes it possible for the voter to inspect his votes as stored within the voting system.

1 Introduction

In 2004, the Ministry of Local Government and Regional Development in Norway mandated a working group to work out a recommendation concerning the future of electronic elections in the country. The result of this work is documented in the report [KRD2006]. The basic conclusions are that there is no need to rush into electronic voting and that electronic solutions should be introduced with great care, due to the current deficiencies in the technical platform. Yet the working group recommended the setup of a project group and a step-by-step introduction of e-voting for certain types of elections. However, we do not know when the solutions proposed in this paper will be turned into reality, or whether they will be realised at all.

The working group rather quickly arrived at the conclusion that it had little value to put electronic solutions into the polling places – the ultimate goal had to be to give the voter the possibility to vote in uncontrolled environments from his home or at work. The particular solutions described in this paper is recommended as the basis for a possible system for Internet-voting in uncontrolled environments, as an alternative to solutions built on trustworthy platforms which may show up in the future.

The working group has been very well aware of the Recommendation No. R (2004) 11 of the Committee of Ministers to member states on E-voting [Rec2004] (later in this paper referred to as "the Recommendation"), and maintain the point of view that the proposed solutions are compatible with its intentions, although perhaps not always with its lettering.

Readers familiar with the Estonian electronic voting system [Maaten2004] [NEC2004] will find a lot of similarities. However, it may be of interest to know that the working group did arrive at similar principles before obtaining detailed knowledge about the Estonian system.

2 Two important principles

The solution proposed in this paper relies heavily on two fundamental principles: The principle of two-phase voting and the principle of repeated vote-casting.

2.1 The principle of two-phase voting

Elections in Norway have for a long time been carried out in two phases: One advanced voting phase followed by the Election Day itself. Between the two phases there is a one or two day break. During this period, the voters who have voted during the first phase will be marked in the Voter register, so that this information is available for the election officials on Election Day.

We propose to continue with this two-phase setup. Electronic voting should be used only in the first phase, voting on the Election Day should be done in the traditional way by means of paper ballots. This gives the voters complete freedom in how to vote, electronically or by paper ballots. At some time in the future, electronic voting may become so popular that the efforts for setting up traditional elections will be reduced to almost nothing. This is feasible; however, it will be driven by the preferences of the voters, the politicians and the society in general, not by the technology.

2.2 The principle of repeated vote-casting

The Recommendation [Rec2004], paragraphs 5 to 8, states the obvious democratic rule that a voter should give only one valid vote in each election event (one person – one vote). An electronic system may enforce this rule in two ways, either by invalidating the voter's credentials for further voting in the same election event, or by letting the vote-receiving server in some way keep track of the identity of the voter and reject multiple ballots from the same voter. The first solution is susceptible to conscious or unconscious errors and mistakes on the client side. Hence, it is better to let the server side handle the duplicate ballots from the same voter. We propose to let the vote-storage server store all the received ballots, rather than rejecting the second and the following ballots. At the end of the voting period, the election system will run through the ballots and only the last ballot received from each voter will be transferred to the electronic ballot box. Thus, the voter may effectively regret and cancel his vote just by casting another one at a later point in time.

As a final possibility for repeated vote-casting, the voter may show up on the Election Day asking to vote by means of a traditional paper ballot. In that case, the election officials will register with the vote-receiving server an instruction to throw away all the electronic ballots cast by the voter during phase one.

The principle of repeated vote-casting reduces significantly the well know democratic concerns connected with voting in uncontrolled environments [Maaten 2004]. There will be no market for buying and selling votes, since the buyer can never know whether the voter will cast another vote, maybe even on the Election Day. And the voter who feels subjected to coercion (e.g. "family voting") may cast another vote as soon as the coercer has disappeared. As we shall see, the principle also makes it possible to allow the voter to check the content of his electronic ballot as it is stored on the vote-storage server, since an observer can never know whether this ballot will be the final one.

3 Raising trust by securing the electronic voting system

Whenever communicating over an insecure channel, the demands for security must be built into the applications *using* the insecure channel. Basically, the sender may send a certain amount of redundant data with the message so that the receiver can check the consistency of the data and ask for retransmission if something seems to be wrong, or the receiver may reflect back to the sender its understanding of the message so that the sender can check that the receiver understood the message correctly.

The weakest point in an electronic election system based on voting in uncontrolled environments is probably the client machine, which may be infected by viruses and other malicious programs. The most difficult part to control is the very first part of the journey of a message from the keyboard to the program handling the input from the keyboard. We can not rule out the possibility that some illegal program is sitting between the keyboard and the rest of the system, faking correct looking screen images but sending completely incorrect data to the vote-receiving server. The only (almost) secure way to compensate for this threat is to have the user enter some redundant data via another completely separated and independent channel, for example via SMS on a mobile phone. The user friendliness in such a setup, however, is questionable.

It is more appealing to let the system reflect back to the voter so much data that the voter is convinced that the vote has been correctly registered. In this way, we utilise two different channels between the mind of the voter and the system: The typing on the keyboard and the visual observation of the reflected data on the screen.

It is, however, important that the reflection of the data is not done by an untrusted client machine, but by a trusted, well controlled server. In order to rule out the possibility that the client may intercept the reflected data and make it look right even if it isn't, the data may be returned to the voter via a completely different technical channel, for example SMS on a mobile phone.

The voting client in the system described in this paper is assumed to be a client machine. However, with the emergence of smartphones, GSM telephones equipped with WLAN access, 3G networks and more and more sophisticated mobile terminals, it is feasible that the voting client is a mobile handset. The advantage is that each of these is equipped with a GSM SIM card or a USIM card upon which the user's ID and PKI functions and key pair can be generated and safely contained. Note that in this case, access to the (U)SIM is secured by PIN and PUK, and the users private key never leaves the (U)SIM, see [THJ2004] for details regarding PKI on the (U)SIM.

3.1 The double envelope principle

In order to be able to allow recasting of votes, some kind of voter identity has to follow the ballot until the last, counting ballot is eventually dropped into the electronic ballot box. At the same time, in order to keep the vote secret, the identity of the voter and the content of the ballot must not be made available to anybody at any time. To ensure this, we propose to use an electronic double envelope setup similar to the one used in the Estonian election system [Maaten2004].

We employ two sets of key pairs for asymmetric cryptography. The first set consists of the public and private key of the voter[1]. The second set consists of the public and private key for the election event. In addition, we will also employ a session key in a symmetric cryptographic process.

As soon as the voter has finalized his electronic ballot and is ready to send it to the vote-receiving server, the client will generate a random session key and perform a symmetric encryption of the ballot. Then the session key is encrypted with the public key of the election event. The message consisting of the encrypted vote together with the encrypted session key corresponds to a paper ballot in a sealed inner envelope.

Normally, this two-step encryption process, called hybrid crypto, is used just for efficiency reasons, since symmetric crypto-algorithms are much quicker than the asymmetric ones. However, in our scheme, the hybrid crypto is also used for another purpose, as we will see.

Next, the client will digitally sign the message with the private key of the voter. This signed message corresponds to an outer envelope containing the already mentioned inner envelope. To the message, we attach some data which in some way gives the identity of the voter.

The whole package is then sent to the vote-receiving server, which will relay it to a firewall-protected vote-storage server where it will be written to a write-once-medium. Further ballots in double envelopes from the same voter will be written to the same medium, and not overwrite previous ballots. The same will happen with a message from an election official saying that all ballots from the voter should be cancelled. At the end of the election period, the election system will pick the last received ballot (if no cancelling message exists), remove the outer envelope by using the public key of the voter to check the signature on the data (the ballot) and, if verified, drop the inner envelope with the ballot in the electronic ballot box. From this point, there is no connection between the identity of the voters and the content of the ballots. The anonymous enveloped ballots will then be unsealed by decrypting the session key with the private key of the election event (which until then is kept secret inside a security module) and then decrypting the message with the session key.

---

[1] It is preferred that this key pair is used for much more than just electronic voting – the best solution is that the key pair is a part of an officially recognised PKI-system. This will reduce the possibilities for that the voter is selling the key pair.

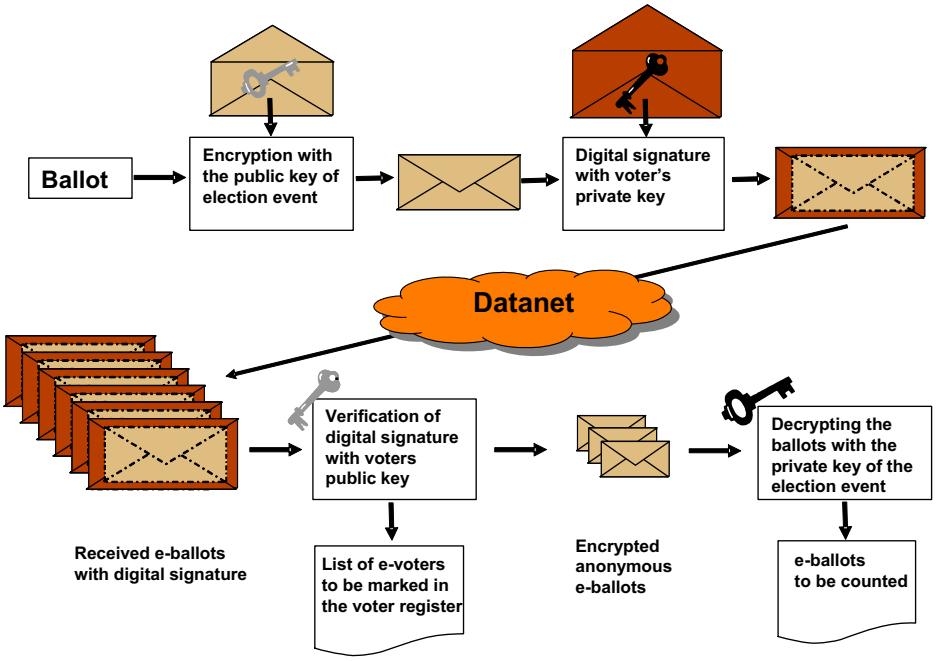


Figure 1: The double envelope principle

3.2 Letting the voter check the ballot

Returning to the question of how to convince the voter that his vote has been properly received, we propose that the doubly encrypted vote is returned to the voter client from the vote-storing server. In this case, the vote-storing server should sign it so that the user is convinced that the vote-storing server is actually storing the ballot. We also propose that the voter at any time during phase one of the election event may request the vote-storing server to send the doubly encrypted ballot to his client.

To be able to decrypt his ballot, the voter must have stored the session key used during voting somewhere. He may have written it down (not very likely), or stored it on a removable storage unit like a memory stick. To store it on the hard disk of the voting client is not to be recommended, for obvious security reasons. With the session key, it is possible for the client machine to open the two envelopes and show the voter the content of his ballot. The outer envelope is opened by decrypting with the public key of the voter, the inner envelope is opened by decrypting with the session key (we are of course not interested in the encrypted session key). The sceptical voter may do this on a client machine different from the one he used for voting – the likelihood that some evildoer may have managed to infect both machines with malicious software that even must show a consistent behaviour, is very small. In the future, this decrypting process may even be done by a mobile phone, so that the voter can use different technical channels for voting and for checking the ballot.

It may well be argued that this functionality is in conflict with paragraph 51 of the Recommendation [Rec2004], stating that ”A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.” If the voter, for any reason, wants to do it, he may show the content of his ballot to anybody, print it or e-mail it, just as he wish. The answer to this objection is of course that the voter may choose to cast another (and maybe completely different) vote at a later stage. Hence, seeing a copy of a ballot stored on the vote-storing server says next to nothing about how the voter finally is going to vote.

The second part of building the voters trust, namely that the final ballot will be dropped in the electronic ballot box, kept anonymous and properly counted, must be solved in a completely different way. The solution here is to use carefully designed and programmed software; verified and certified by an accredited certification institution. Additionally, if deemed necessary, the whole process may be run in parallel on different machines with different software developed by different developers with different methods, and compare the results – so called N-version systems [Liburd2004]. This is possible because this part of the election process can be run on a very limited number of machines in a heavily controlled and secured environment.

3.3 Keeping the votes anonymous

The anonymity of the votes (the impossibility of connecting the content of the ballot to the identity of the voter) rests on the principle that the double enveloped ballots and the private key of the election event should never be available to any person at the same time. Since it is difficult to keep the distribution of the double envelopes stored on the vote-receiving server under complete control (they may be logged for security reasons, or perhaps even copied by a hacker misusing the available functionality for checking the ballot), the solution is to handle the private key of the election event very carefully. It should be stored in a security module (separate hardware container) until it is time to open the inner envelopes, and it should be disposed of as soon as this task is done. In this case, a pin code may also be required in order to enable use of the key.

The degree of anonymity possible with a traditional paper ballot system cannot be guaranteed by an electronic voting system, however, these and other technical means can be employed to guarantee anonymity as far as possible. A security audit is essential to be able to track whether or not the election event key is being misused at any time.

If this solution does not look trustworthy, additional security may be achieved by using voter pseudo-identities. This, however, complicates the task of getting hold of the public key of the voter when opening the outer envelope and the latter solution has therefore not been recommended by the working group.

4 An overall picture of the architecture

Figure 2 depicts the overall architecture of the voting system. In the complete report written by the working group [KRD2006], the functionality of each module is described by means of UML Use cases.

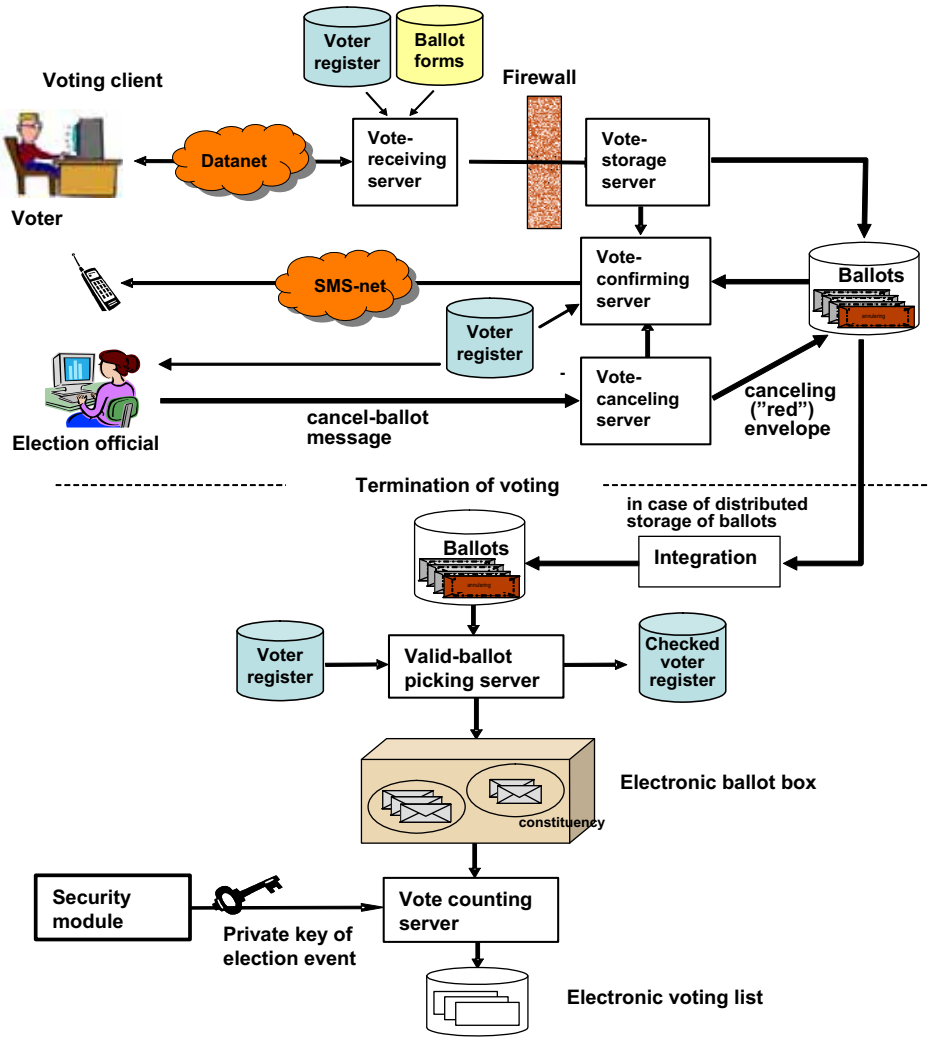


Figure 2: The architecture

5 Other security issues

Securing the availability of the vote-receiving server and other entities involved in the process is essential for the electronic voting to be conducted fairly. It is crucial to ensure that the vote-receiving server does not go down – in particular on the last day. Actually, last year the electronic tax return system in Norway failed to deliver on the last day [Ryv2005], and as a consequence, the deadline for submitting tax returns was extended by one day. For that service this was acceptable to the public, but would the citizens accept such a delay in e-voting? An issue related to this is protecting the vote-receiving server from so called denial of service (DoS) attacks aimed at making the vote-receiving server unavailable. Therefore we envision that a complete election system will encompass several vote-receiving servers, located in different geographical areas. On the other hand, we may have only one vote-storage server, but with well developed backup facilities.

The availability of the underlying network must be also be secured – attacks on parts of the network to take down network segments in order to prevent voters from being able to cast their votes should be anticipated. In a close election, targeting specific neighbourhoods that are known to favour the opposing side by e.g. flooding the local network to prevent votes from being cast electronically is easily carried out. This risk can be mitigated by the solution presented in this paper under the assumption that it is difficult to ascertain when voters will cast their votes. However, traffic analysis over several elections might reveal information on how likely it is that voters cast their votes ahead of time instead of waiting until the last day – one can predict that most people will wait until the last day to cast the final vote. In this case it should be expected that sabotage by creating denial of service attacks targeting the voting traffic may be widespread. Preventing this type of sabotage will be challenging, as known attacks may be easy to prevent, but new and effective attacks may come as a surprise, making it difficult to even mitigate the attack. We only have to look at the example of sabotage of the "Get out the vote" operations regarding organized phone jamming during the 2002 Senate race in New Hampshire in the United States [Coh2006] to get a flavour of how easy it may be to attack the underlying network. A very big concern with this type of sabotage carried out in a broadband network (both fixed and mobile) is that it may be difficult to discover, and the extent of the sabotage may not be uncovered until long after the election results have been certified.

This is only one example of electronic vote sabotage. For the system described in this paper, sabotaging the electronic vote system by attacking the underlying untrusted network should be considered carefully. For example, in a broadband IP-based network it may be easy to prevent users from voting electronically or prevent the ballots from arriving. This type of attack is of course easily discovered by the user, but if the user does not anticipate that this may be a problem and waits to the last minute to cast his/her vote electronically, he may be forced to go the polling place the over next day.

The attack scenarios discussed here show that it is difficult to ensure that voters will have completely equal access to the electronic voting system.

6 Conclusions

We are of the opinion that an e-voting system based on the principles described in this paper has the potential of being universally trusted by the voters, the election administrators, the politicians and the society in general. The principle of repeated vote-casting alleviates the well known democratic concerns with electronic voting in uncontrolled environments. At the same time, it allows for the voter to inspect his ballot as it is stored on the vote-receiving server without threatening the secrecy of the final and counting vote. In order to make it possible for the voter to decrypt the doubly enveloped ballot, the session key used during vote casting must have been stored on some medium, for example a memory stick. In order to build trust to the part of the system which is picking the valid votes and counting them, this part of the system should be designed and programmed very carefully, and verified and certified by an accredited certification institution. If deemed necessary, the whole process may be run in parallel on different platforms and the results compared (N-version system). However, it will still be difficult to ensure that voters will have completely equal access to the e-voting system.

References

[Coh2006] Cohen, A.: *A small time crime with hints of big time connections lights up the net*. http://www.nytimes.com/2006/04/17/opinion/17mon4.html?_r=3&oref=login&pagewanted=print&oref=slogin

[KRD2006] Rapport: Elektronisk stemmegivning – utfordringer og muligheter. Kommunal og regionaldepartementet 2006. (In Norwegian – an English version will follow.) http://odin.dep.no/krd/norsk/dok/andre_dok/rapporter/016051-220022/dok-bn.html

[Liburd2004] Liburd, Soyini: *An N-version Electronic Voting System.* Caltech/MIT Voting Technology Project Working paper # 17, July 2004 http://vote.caltech.edu/media/documents/wps/vtp_wp17.pdf

[Maaten2004] Maaten, Epp: *Towards remote e-voting: Estonian case*. In Prosser & Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society. Proceedings, Gesellschaft für Informatic 2004. http://www.e-voting.cc/files/E-Voting-in-Europe-Proceedings/

[NEC2004] The National Election Committee: *E-Voting System – Overview* http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

[Rec2004] Recommendation No. R (2004) 11 of the Committee of Ministers to member states on E-voting

[Ryv2005] Ryvarden, E.: *Skatte-servere tålte ikke trykket*. Digi.no, April 30 (2005) (in Norwegian)

[THJ2004] Johannessen, Tor Hjalmar: *On the mobile, its security issues and applicability potentials.* Teletronikk, 100 (1), ISSN 0085-7130, 2004.

Session 5: Redesigning Workflows for Electronic Voting

A generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process

Alexandros Xenakis, Ann Macintosh

International Teledemocracy Centre
Napier University, Edinburgh
{a.xenakis | a.macintosh}@napier.ac.uk

Abstract: In this paper we suggest a generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process. Based on the hypothesis that the electoral process has been through a "silent" re-engineering phase, we present the process re-engineering concepts which can be used to depict the redesign of the electoral process to an e-electoral process through the use of ICTs. Following we provide a five stage outline of the suggested re-engineering methodology. Finally we discuss the benefits of its implementation and suggest areas for its prospective application.

1 Introduction

The purpose of this paper is to present the process re-engineering concepts which can be used to depict the redesign of the electoral process to an e-electoral process through the use of ICTs and more importantly suggest a generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process. The paper is based on a completed doctoral research founded on evidence deriving from the case of the 2002 and 2003 UK e-voting pilot schemes. Reflecting the UK government's intention to develop "the capacity of holding an e-enabled general election some time after 2006" [HG 02] (p.47), 16 local authority legally binding e-voting pilots took place on May 2002 followed by 20 more pilot schemes held during the local authority elections on May 2003. This research addressed the following overarching research question: *"What are the non-technical constraints in re-designing the electoral process in relation to ICTs?"*

The analysis of the e-electoral process conducted, was based on the hypothesis that the electoral process has been through a "silent" re-engineering phase. That had lead the authors to adopt a process stage approach for its analysis and suggest the use of process re-engineering methods to support its future deployment [XM 03a, 03b]. However, no evidence has been identified to suggest that any kind of organized re-engineering attempt of the traditional electoral process has been undertaken prior to the deployment of the UK e-voting pilots. According to the UK Government, future e-enabled electoral processes and services could be deployed in relation to [HG 02]:

1. Elections to the Westminster Parliament
2. Elections to the Scottish Parliament
3. Elections to the Devolved Assemblies (Wales and Northern Ireland)
4. Elections to Local Councils
5. The conduct of referendums
6. Private ballots under statutory control
7. The on-line registration of voters
8. The on-line application to be an absentee voter.

All the above electoral processes present many differences between them in terms of surrounding legislation, electoral system used, political importance, social background of the electorate and its resulting electoral behaviour.

2 The use of process re-engineering in government provided services

Electronic voting is an interdisciplinary field of research based on the collaboration of a number of well established scientific fields. Computing experts need to co-operate with sociologists, political scientists, and media communication experts. Moreover, e-voting research particularly requires the contribution of legal and public administration experts. E-elections, similar to traditional elections, are government owned and initiated processes, and as such, many of the activities involved in their undertaking are closely related to public administration, in this case electoral administration in particular. In the past, process re-engineering in the public administration sector has been widely used to re-organise other administrative processes that had to be redesigned due to the introduction of ICT in some or all of their stages. Thaens [TBD 97] has discussed the use of BPR (business process re-engineering) in the case of taxation. Bellamy and Taylor [BT 97] have referred to the use of adaptive information systems in the case of the UK Criminal Justice System. Pollard [Po 97] has analysed the case of organisational transformation of the National Mapping Agency of Great Britain. Willcocks [WCJ 97] provides detailed analysis of three cases in the UK related to the healthcare sector and the postal service. Van Belle [VB 97] discusses the case of re-engineering the Flemish Department of Education with the purpose of introducing ICT. Lenk [Le 97] has explored the enabling role of ICT in relation to the risks and opportunities involved, stating the need for continuity of structures of accountability. Pratchett [Pa 97] focuses on the use of BPR at the local authority level, referring to the level of radical re-engineering, the suitability of processes to undergo re-engineering and the level of dependence on ICT. Zuurmond and Snellen [ZS 97], on the other hand, take a more managerial approach discussing organisational structures and informational architectures within the bureaucratic paradigm.

In this paper the authors suggest the development of a generic electoral re-engineering methodology. Such a methodology has the potential to support the structured re-engineering of any electoral process providing a fit for purpose approach based on the experience gained to this date.

3 Research methodology

Initially, BPR concepts are used to assess the redesign of the electoral process to an e-electoral process and analyse the resulting effects on the validity of the process, the effectiveness of its administration and the social acceptance of its results. In the past, process re-engineering in the public administration sector has been widely used to re-organise other administrative processes that had to be redesigned due to the introduction of ICT in some or all of their stages. However, it was necessary to adapt the process re-engineering rational to the characteristics of the particular process analysed, which in this case is the electoral process. The challenge was to identify the different sub-processes (stages) that take place within an e-election and decide which process re-engineering concepts can be beneficially used in their analysis.

The purpose of the following section is to present the BPR concepts used to depict the redesign of the electoral process to an e-electoral process through the use of ICTs and analyse its resulting effects. To that effect a review of existing BPR methodologies was conducted in order to identify the key BPR concepts which can support the analysis of the e-electoral process. The theoretical BPR concepts presented hereafter form the basis of the process stage approach to the e-electoral process adopted in this paper. The main BPR concepts used are:

- Agent roles and their procedural responsibilities
- Agent accountability and agent obligations
- The definition of agent dependencies
- Multiple agent communication, co-ordination and control

All of the above concepts have been useful for the analysis of the three non-technical aspects of e-voting explored during this doctoral research. Defining, and re-defining agent responsibilities was used for the analysis of the trust relationships developed between agents to support the social acceptance of the e-electoral process. Defining agent accountabilities was used for the analysis of the procedural security aspect of e-voting. Finally defining dependencies and exploring how multiple agent communication, co-ordination and control mechanisms can be applied in the deployment of e-voting was useful for the analysis of the e-electoral administration.

4 Essential BPR concepts used for the analysis of the e-electoral process

This section provides a reference to the essential BPR concepts which can support the analysis of the e-electoral process.

- Defining agent roles and their procedural responsibilities

Roles are related to agents who operate under an obligation to fulfil certain responsibilities. Simple actions are assigned to agents through roles. Processes are composed from the combination of these simple actions. Roles define an agent's state at any point in time. Agents rationally choose their next action according to the options associated with each specific role [Hi 85]. The description of e-voting agent roles can serve the detailed allocation of tasks attributed to each agent. This aspect mainly aims at the allocation of procedural responsibilities but also enables a better understanding of the overall process.

- Defining agent accountability and agent obligations

The notion of agent accountability is closely related to the identification of responsibilities. A person is held accountable by others in relation to the fulfilment of one's responsibilities, which will in turn create procedures even if not originally defined [Sc 93]. By identifying agent responsibilities one can also identify their procedural obligations. Obligations limit the choice of action, and therefore need to be fulfilled according to the undertaken responsibilities. Responsibility is 'for' something; obligation is 'to do' something. Obligations are concerned with keeping things the way they are or changing them in relation to the responsibility held [DM 89]. The satisfaction of obligations is achieved by the introduction of rules which constrain agents' actions. Rules are therefore constraints put on people by the organization on how they should act [Ou 92]. Constraints are thereafter inherited by processes and activities either partially or in full. In the e-voting context, business rules are substituted by the existing legal framework defining an election, as legislation varies according to different elections. We should therefore consider the relevant legal issues as a dynamic factor to which e-voting deployment should adjust accordingly.

- Defining dependencies

When agents participate in contractual relationships, they undertake a set of responsibilities that are determined by the terms of any given contract. Within an organization, contractual (responsibility) relationships determine the type of the structural relationships between pairs of co-workers whereas, a contractual relationship between an external agent and an organization exists only for the duration of a specific contract. The notion of contractual relationships is broadly used by the UK civil service where independent agencies provide the central government with their services therefore developing a contract between them [HT 88]. The analysis of contracts will in turn help identify agent responsibilities and dependencies among them, deriving from their participation in contractual relationships. Once agent responsibilities have been identified they can subsequently be allocated along the e-voting process. Defining dependency relationships between the different collaborating parties in the e-voting procedures can be achieved by clearly demonstrating each agent's role and internal responsibilities. The focus should be on the identification of dependencies that are critical for the election success.

- Enabling multiple agent communication, co-ordination and control
According to Mintzberg [Mi 89] there are six types of coordination mechanisms:

1. Mutual Adjustment (informal communication)
2. Direct Supervision (common supervision of people whose work is related)
3. Standardization of the work processes (when different tasks involve different people in one process)
4. Standardization of outputs (specification of expected results)
5. Standardization of skills (based on the training of the people involved in the process)
6. Standardization of norms (describing a process so that everyone involved has the same understanding of it)

The co-ordination of the agents involved in the delivery of electronic voting is of central importance due to their multiplicity and the complex nature of the multiple channel e-voting process.

5 A five stage approach to electoral process re-engineering

The following sections provide a five stage outline of the suggested generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process.

5.1 Understanding the context of the existing electoral arrangements and the aspirations of the main government organisations concerned

The first stage of e-electoral redesign is a diagnostic one. The aim is to have a full understanding of the electoral process which is going to be re-designed to an e-electoral process. Initially, one has to identify the government agents involved in the voting procedures. Related government agents should be approached for data which will be later used for both modelling and analysis of the process. The primary aim is to gather internal data, in any form (previous e-voting evaluation reports, statistics, cost calculations etc.). Organizational data could also be collected from a variety of internal sources.

That should be followed by interviewing representatives of these agents. When conducting interviews with the government organisations' departmental managers, one should try to identify opportunities for improvements and understand the organisations' culture. These interviews will also identify further data collection opportunities and determine the focus issues which will constrain the re-design of the process. Interviews should however be focused on identifying:

- Each related department's tasks, responsibilities and activities in relation to the electoral process
- Expected inputs and resulting outputs related to the above activities

- Input suppliers and output customers for these activities, whether internal or external
- Formal and informal communication lines

After concluding the above practices a decision has to be taken by the main government organization concerned as to whether re-engineering will be aiming at process improvement (an e-enabled paper ballot based election) or process innovation (an e-voting process possibly including an e-enabled element as well). This would derive from the combination of the opportunities identified in the earlier steps and the aspirations of the government organisation, meaning the amount of risk they are willing to take.

In the final part of this stage, once the data has been gathered and evaluated and the decision on the aim of the re-engineering has been taken, a document should be prepared containing the specific objectives of the re-engineering effort.

5.2 Modelling (who, what, where and how)

The modelling of the existing and proposed electoral process will be based on the information gathered in the previous stage. The primary concern when modelling the processes is to:

- Further analyse the agents involved into macro agents and micro agents. According to [Jo 89] micro agents are individual persons whereas macro agents are entities like organizations and companies. Macro agents have micro agents as parts.
- The identification of agent roles and resulting responsibilities
- Identification of critical contractual relationships between agents involved in technology provision contracts, authority contracts in bureaucracies (administration contracts) and long term unwritten contracts within groups based on principles of mutual latent trust.
- The identification of objectives, interactions and dependencies resulting from the above contracts
- The fragmentation of processes into stages including smaller operation and activities
- The identification of coordination and control mechanisms
- The explicit identification and statement of rules (whether legal or otherwise) limiting all the above

Three basic model constructs are suggested:

- Process stage modelling (what needs to be done and when)
  By modelling each stage of the electoral process, one can monitor the parallel activities taking place concurrently. Such models can be used to describe the activities taking place (what needs to be done) in the different stages of the e-electoral process (and when). Representing agents within the process stage models would extend their descriptive functionality.

- Contractual relationships modelling (who should deliver what and who expects what)
  The contractual relationships perspective could be modelled so as to identify the obligations of each agent towards others (who should deliver what) and accordingly the deriving dependencies of deliverables between agents (who expects what)

- Agent role modelling (how should agents act)
  The focus of these models should be on roles, activities and the agent responsibilities deriving from those activities. The question here is to define how the agents identified should respond to their responsibilities (how should agents act) within their combined activities which produce the overall electoral process.

5.3 Analysis (why)

The purpose of the analysis of gathered data, existing and proposed models, is to understand why process stages, contractual relationships and agent roles are executed in the way identified. Analysis tools and methods can either be developed or alternatively **adapted as appropriate from those having already been used in the re-engineering of** business processes. A set of analysis methods which have been used in BPR and could potentially prove useful for the analysis of the e-electoral process include:

- Analysis of the abstraction level of the prepared models, testing for clarity and transparency [IH 92].
- Principal-Agent analysis of the contractual relationships related to agent co-ordination, management and control [FJ 83]
- Management structure analysis to evaluate the use of management resources, by looking at issues such as span of control and layers of management [BC 91].
- Mission/non- mission analysis to assess whether an agent's obligations are critical to the achievement of the process objectives [Gl 94].
- Fragmentation-concentration analysis to define the number of full time equivalent employees needed to undertake an activity, in this case related to the issue of costs and the number of staff needed for the deployment of e-voting [Ha 90], [DS 90].
- Fractionalisation analysis to establish the level of fragmentation of an employees work and consider whether the responsibilities undertaken by each agent are correctly allocated to the agent in question according to time and expertise [Gl 94].

At the end of this stage one should have a full understanding of the current electoral arrangements, the proposed changes to the electoral process and the resulting effects that these changes would incur in terms of security, administration and social acceptance of the e-electoral process.

5.4 Re-design

In this stage the conclusions reached in the analysis undertaken in stage three, together with the proposed would-be models, and the models of existing electoral arrangements produced in stage two should be presented to the main government agent holding the election. A second round of interviews, this time including more junior employees could identify further opportunities for improvement and validate those already identified. Employees should be asked to contribute to the validation of the would-be models before those are applied so as to finalize them.

The internally gathered data could be supplemented by external data about known best practice on the deployment of e-voting. However this should be relevant to the specific objectives of each re-engineering exercise. If for example the aim is to introduce a certain type of e-voting technology then one should look into past experience using the same kind of technology. Nevertheless, e-voting is still at a pilot stage and accumulated best practice is hard to identify for two main reasons. Firstly there is little experience in large scale e-voting deployments. Secondly, in order to define best practice one has to set commonly accepted evaluation criteria, or at least accepted in the context of a specific re-design effort. Widely recognized best practice will take a certain amount of time and testing to develop in the e-voting environment.

The outcome of this stage should be a re-designed e-electoral process, the re-design solutions being based on the organised introduction of ICT in the traditional electoral process.

5. 5 Continuity of e-electoral redesign

This last stage should be concerned with maintaining the benefits gained during the re-design effort. The necessity for adaptation to e-voting technology advances, as well as to changing voter trends, fosters the necessity for repetitive process improvement. Continuous staff training should also be undertaken, responding to the need for additional technical, procedural and managerial skills. This doctoral research produced three separate analytical methods for the evaluation of e-electoral processes which could serve the continuous assessment of e-voting schemes:

- Procedural security analysis [XM 04a], in which given security constraints are used as evaluation criteria to measure the existing or prospective security level of e-electoral procedural practices
- Trust flow analysis [XM 04b], a method which provides an abstract representation of how stakeholders interact in terms of trust within the scope of a re-designed electoral process
- Level of difficulty analysis [XM 04c], which evaluates the expected level of difficulty of a suggested e-voting scheme prior to each implementation based on specific criteria.

6 Conclusions

Defining roles and responsibilities within the e-voting process could provide a better understanding of who is responsible for doing what in the different process stages so that the election result is produced. Transparency of operations could provide a better insight of agent interactivities. Thus, the comparative analysis of agent roles between the traditional and the new e-electoral process could be used to specify how agent responsibilities and obligations are altered and re-distributed due to the introduction of ICTs in the electoral process. This in turn supports trust analysis and social acceptance [XM 05].

Procedural risks such as user errors could be identified in the analysis of the e-voting process and therefore either predicted or counter-measured in a way that the outcome of the process would not be endangered. The identification of procedural security gaps which could foster fraud opportunities and their allocation to specific process stages could function as a preventive mechanism against the possibility of fraud in all its different forms. Hence this line of research would support preventive management of e-voting fraud.

Better management could be provided by identifying the opportunities for effective administration of the introduced e-voting technologies. This is in line with the requirement for customisation of e-voting technology to fit local needs and the need for common evaluation criteria on the effectiveness of e-voting technology. The stage analysis of the e-voting process could also prove beneficial in the effective allocation of resources by indicating the optimal combinations of resources in parallel process stages of the multiple channel e-voting process. Finally, the re-engineering of the process could lead to process simplification, which is also a necessity in the deployment of e-voting.

7 Future work: Investigating cost efficiencies for e-voting

The matter of cost is considered to be a defining factor in the deployment of e-voting in all major e-voting reports related to the UK context [Co 02], [Pa 02], [FR 02]. Government organisations need to manage the economic risk of investing in e-voting technology and make a return on their investment. According to the Electoral Commission one of the main reasons for piloting e-voting was to establish whether cost efficiencies can be achieved. Although a lack of a specific methodology to measure and evaluate the cost of all the different e-voting channels and their combinations is formally acknowledged, the Commission does consider paper ballot e-counting as having established its related cost efficiencies, hence the limited number of e-counting pilots in the 2003 pilot schemes [Ec 03]. A further issue is the documentation of the experience gained in this area. Although detailed evaluation reports have been produced with regard to technical, security, legal and accessibility issues, to this date no detailed study has been published with regard to e-voting costs.

The deployment of electronic voting systems requires considerable initial investment, operation and maintenance costs. Alternative combinations of e-voting or e-enabling technologies can result in different financial requirements. The authors therefore suggest that future research is oriented towards producing a cost accounting methodology aiming at estimating and controlling multiple channel electronic voting costs. There is an apparent need to define specific cost metrics so that when one refers to the costs of e-voting there is mutual understanding. Such research would answer e-voting costs criticism which is fostered by the absence of specific cost metrics. The authors also suggest that any cost methodology should not cover e-voting channels alone, but the combination of e-channels with paper-based channels (postal and polling station voting). If a process stage approach is adopted for all the different channels, then common costs can be identified and economies of scale can be calculated for different combinations of multiple channel elections. Possible cost reductions could be identified by allocating costs between the different stages, agents and objects involved in the process. The modelling of the e-voting process could also prove beneficial for the optimum allocation of resources, by representing the alternative options of allocating resources between the parallel stages of different voting channels. Future pilot projects offer an excellent opportunity for such a study according to the scale and the nature of the pilot, providing that precise cost estimates and final costs are kept during the pre-electoral period in a concise, pre-defined format.

The cost deriving from the adoption of e-voting systems and whether this can be considered as justifiable is a matter of policy. In one of the interviews held during the fieldwork of this doctoral research with the Returning Officer of the UK local authority where observations of an e-voting scheme were undertaken, the RO expressed the following opinion on the matter of cost:

*"In the issue of setting this (*e-voting adoption*) in priority to other priorities, when you've got basic services that need to be delivered, it means that members (*local councillors*) will have to take a very long hard view"* adding that *"if they have to make a choice between whether they spend money on the voting structure as opposed to spending money on street lights then it becomes a very difficult choice"*

E-voting costs nevertheless should be measured against the expected added value that their deployment will incur in the wider democratic process. Usually, the prospective benefits from the introduction of e-voting technologies are related to the hypothesis that the convenience offered can be used as a counterbalance against voter apathy and therefore increase voter turnout, which in turn legitimises the outcome of the electoral process. A further hypothesis is based on the assumption that young voters who are familiarised to the use of technology in general, are more inclined to participate in the electoral process if presented with the opportunity to use technological means to cast a ballot. However both of the above assumptions remain to be proven. Eventually, if no apparent relationship between e-voting and increased voter turnout is achieved, then the future of e-voting will lay solely upon the cost factor as far as the state is concerned and the trust factor from the voters' point of view.

References

[BT97] Bellamy, C. & Taylor J.A. (1997). Transformation by Stealth: the case of the UK Criminal Justice System. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 37-54, IOS Press.

[BC91] Butler-Cox Foundation (1991). The Role of Information Technology in Transforming the Business: Management Summary, Report 79, January 1991.

[Co02] Coleman, S. & Independent Commission on Alternative Voting Methods (2002). Elections on the 21st Century: from paper ballot to e-voting. Electoral Reform Society.

[DS90] Davenport, T.H. & Short, J.E. (1990). The new industrial engineering: Information technology and Business Process Redesign. *Sloan Management Review* vol.11.

[DM89] Dobson, J.E. & McDermid, J.A. (1989). Security models and enterprise models. In Landwehr, C.E. (ed*.) Database Security: Status and Prospects II*, Amsterdam: Elsevier Science.

[Ec03] Electoral Commission (2003). The shape of elections to come: A strategic evaluation of the 2003 electoral pilot schemes, July 2003

[FR02] Fairweather, B. & Rogerson, S. (2002.) Technical Options Report, De Montfort University, Leicester.

[FJ83] Fama, E.F. & Jensen, M.C. (1983). Separation of Ownership and Control*. Journal of Law and Economics* vol.26, pp.301-326.

[Gl94] Glykas, M. (1994). "Agent Relationship Morphism Analysis" PhD thesis, University of Cambridge.

[Ha90] Hammer, M. (1990). Re-engineering work: Don't automate, Obliterate. *Harvard BusinessReview,* July-August 1990.

[Hi85] Hirscheim, R.A. (1985). *Office Automation: A Social and Organizational Perspective*. Chichester: Wiley Series in Information Systems.

[HT88] H.M Treasury (1988). Improving management in Government: The next steps. Efficiency Unit, HMSO.

[HG02] HM Government (2002). In the service of democracy, a consultation paper on a policy for electronic democracy.

[IH92] Ip, S, & Holden, T. (1992). A Knowledge based technique for the process modelling of information systems: The Object Lifecycle Diagram. *In proceedings of the 4th conference of Advanced Information Systems Engineering*. Manchester, UK.

[Jo89] Johansson, I. (1989). *Ontological Investigations: An Inquiry into the Categories of Nature, Man and Society*. London: Routledge.

[Le97] Lenk, K. (1997). Business process reengineering in the public sector: opportunities and risks. In Taylor, J.A., Snellen I.Th.M. and Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 151-165, IOS Press.

[Mi89] Mintzberg, H. (1989). *Mintzberg on Management.*. New York: The Free Press.

[Ou92] Ould, M.A. (1992). Process modelling with RADS*. IOPener* 1(5).

[Pa97] Pratchett, L. (1997). Reengineering UK local government: opportunities and prospects. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 165-188, IOS Press.

[Pa02] Pratchett, L. (2002). The implementation of electronic voting in the UK. LGA Publications, The Local Government Association.

[Po97] Pollard, P. (1997). Organisational Transformation and the commodification of spatial data: a case study of the National Mapping Agency of Great Britain. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 71-89, IOS Press.

[Sc93] Scheer, A.L. (1993). A new approach to business processes. *IBM Systems Journal* 32(1).

[TBD97] Thaens, M., Bekkers, V.J.J.M., van Duivenboden, H.P.M. (1997). Business Process Redesign and Public Administration: a perfect match ? In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 15-36, IOS Press.

[VB97] Van Belle, J.L. (1997). Reengineering administration: the case of the Flemish department of Education. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 133-149, IOS Press.

[WCJ 97] Willcocks, L.P., Currie, W.L., Jackson, S. (1997). In Pursuit of the re-engineering agenda: research evidence from the UK public services. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 103-132, IOS Press.

[XM03a] Xenakis, A. and Macintosh, A. (2003a). Using Business Process Re-engineering (BPR) methods and analysis tools to effectively implement electronic voting. *Proceedings of the 3rd European Conference on E-Government ECEG 2003*, Ireland.

[XM03b] Xenakis, A. and Macintosh, A. (2003b). A Taxonomy of Legal Accountabilities in the UK E-voting Pilots. *Proceedings of EGOV 2003, the 2nd International Conference on Electronic Government*, Czech Republic.

[XM04a] Xenakis, A. and Macintosh, A. (2004a). Procedural Security Analysis of Electronic Voting. *Proceedings of ICEC 2004*, *6th International Conference on Electronic Commerce* Netherlands.

[XM 04b] Xenakis, A. and Macintosh, A. (2004b). Trust in public administration e-transactions: e-voting in the UK. *Proceedings of TrustBus 2004*, *1st International Conference on Trust and Privacy in Digital Business,* Spain.

[XM 04c] Xenakis, A. and Macintosh, A. (2004c). Levels of difficulty in introducing e-voting. *Proceedings of EGOV 2004, the 3rd International Conference on Electronic Government,* Spain.

[XM 05] Xenakis, A. and Macintosh, A. (2005). Procedural Security and Social Acceptance in E-voting. *Proceedings of HICSS-38 Thirty-Eighth Annual Hawaii International Conference on System Sciences*, USA.

[ZS97] Zuurmond, A. & Snellen I.Th.M. (1997). From Bureaucracy to infocracy: towards management through information architecture. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 205-224, IOS Press.

Election Workflow Automation - Canadian Experiences

Goran Obradovic, James Hoover, Nick Ikonomakis, John Poulos

Dominion Voting Systems Corporation
20 Mowat Avenue
M6K 3E8, Toronto, Canada
{goran.obradovic | james.hoover | n.ikonomakis | john.poulos}@dominionvoting.com

Abstract: Democratic parliamentary and presidential voting supported by election systems worldwide represents the essential idea behind any free society. In recent years, numerous challenges have been overcome to satisfy this fundamental principle. On one side we have low voter turnout and high electors migration, on the other, sometimes complex electoral systems such as preferential or transferable ballot voting. In addition, proliferation of modern computerized technologies is giving hope that with new automated processes and voting channels, the election process and democracy as a whole can be more accessible, secure and transparent. In this paper we are presenting the Democracy Suite as the field-proven solutions for full election automation workflow.

1 Introduction

Governments in Canada are organized in a range of geographical structures. The federal government uses a single member plurality system in 308 ridings, also known as electoral districts. Similar systems are used in each province but with lower numbers of ridings. Municipalities use more complex structures – typically electing a single mayor and multiple councilors or trustees using composite ballots with several plurality contests. To date, preferential or transferable ballots have not been widely used but successful pilot projects are contributing to serious consideration. Elections dates in Canada can be divided into two general categories – fixed and variable. Most municipal events are on fixed dates and several hundred towns and cities can have elections on the same day. In contrast, provincial and federal governments are modeled on a parliamentary system so governments can be defeated at any time during a 5-year term.

In Canada, paper ballots and in-person voting are predominantly used for all types of elections. In some cases vote-by-mail is used as well, but in essence this voting channel still uses paper ballots with central vote counting. For decades, the voting process was mostly performed manually – electors were recorded using a hard-copy voters list and ballots were tabulated by hand. This basic system was acceptable for simple elections, but recording inefficiencies cause long line-ups at voter registration and manual vote tabulation leads to inconsistencies and long delays in results reporting.

Automation of vote tabulation has started in mid 1990's and was predominantly used for decentralized and centralized paper ballot processing for local elections in large cities. These first generation systems from Diebold and ES&S, designed before introduction of Voting Systems Standards [FEC02] and HAVA standards [HAVA02], didn't provide accessible, secure and transparent election process as required by [EA05]. In addition, lack of integrated elector management system, standard-based data interchange schemas and alternative remote voting channels, made those systems inappropriate for Canadian elections. Since late 2002, Dominion has been developing an integrated and automated election system under the name of Democracy Suite. This set of software applications and hardware devices, coupled with variety of services, provides a complete set of solutions for traditional in-poll or remote paper-based voting, electronic remote voting (Internet), and elector management. In this paper we will provide a brief technical overview of the Democracy Suite as it was deployed in the variety of elections in the provinces of British Columbia, Alberta, Ontario, Quebec and Newfoundland.

2 Automated Election Workflow

The overall election process schedule is separated into *election event* and *election cycle* activities (Figure 1). Election events represent specific voting occurrences, with its date and the jurisdiction of the given electoral authority, plus a unique set of *election entities*, such as polling divisions, contests, candidates, ballot styles, voting channels, etc. The election cycle activities, on the other hand, include elector management activities for obtaining the complete and most up to date list of eligible voters.

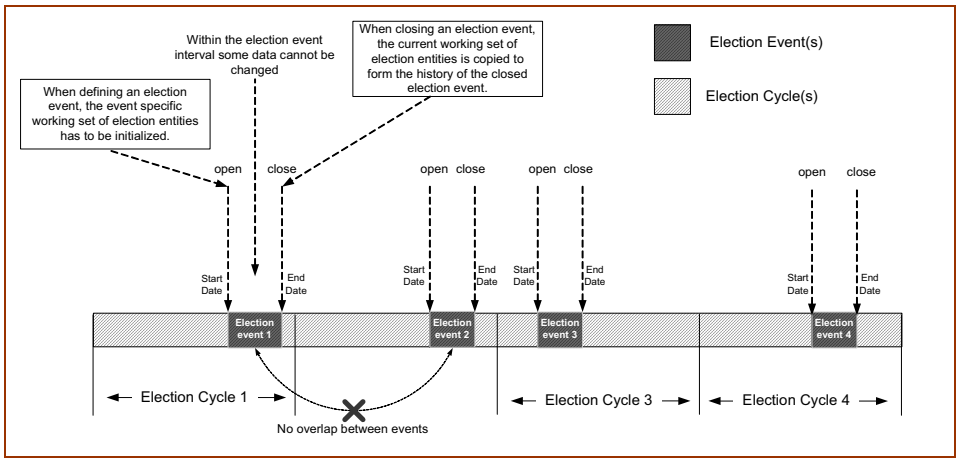


Figure 1: Relation between election events and election cycles.

Every election event begins by collection of election entity data. This election event definition phase primarily involves accumulation of contest and candidate names as well as all additional geographical and administrative information needed (polls, polling districts, polling locations, polling stations, etc.).

This data usually comes directly from electoral authorities responsible for event organization and enters our system in an XML defined schema for election entity information exchange, similar to EML [EML05]. After importing this data into our election event data model, the system proceeds with automated creation of ballot styles, voting information files needed for programming of voting channel devices, and election results reporting XML schemas.

All voting channels utilize a common set of configuration files (channel configuration and voting information files) which contain directives for the system operational and election rules (Figure 2). For data protection and performance issues, these files are encrypted and in binary format. Using this approach, complete and seamless integration of all system components is achieved - unifying diverse entities with clear technical separations (i.e. paper versus electronic ballots). Simply stated, the system provides a) only one point of definition for all relevant election data and b) only one point of tabulation from different voting channels. Figure 2 also shows different voting channels supported by our automated election workflow:

a) Decentralized poll-based voting using paper ballots and polling station tabulators (CF200 series)
b) Centralized voting using paper ballots and central count tabulators (CF500 Series)
c) Electronic remote voting using electronic ballots and Internet (e-Voting)
d) Fax-back remote voting using paper ballots and fax services
e) Vote-by-mail remote voting using paper ballots and regular postal services

Ballots cast, using any of the voting channels, are collected using the same central platform which performs a variety of tasks such as vote tallying, verification, auditing and publishing.

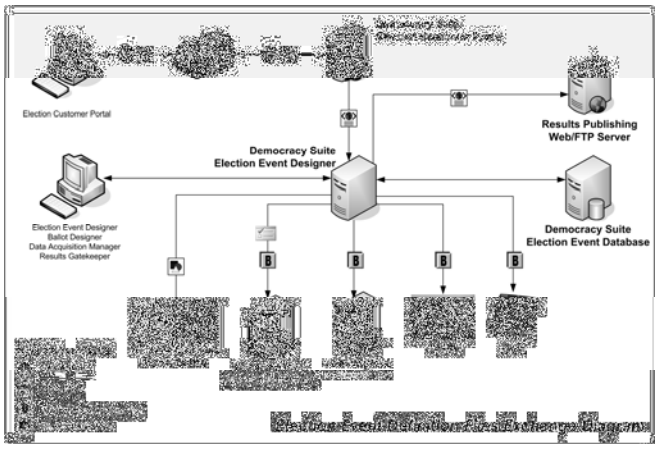


Figure 2: Election event definition files exchange diagram.

In addition, for full support of a variety of voting channels, Democracy Suite includes elector management support for registration and tracking of electors. This support includes day-to-day elector management (add, modify, delete), address management, and

administrative areas management tasks. For real-time voter tracking during election events, Democracy Suite creates an electronic poll-book list of electors which is synchronized with central elector register using GPRS/EDGE or regular Internet connectivity. Finally, the system provides full support for remote voting registration, such as vote-by-mail and Internet voting. Figure 3 presents an elector management deployment scenario.

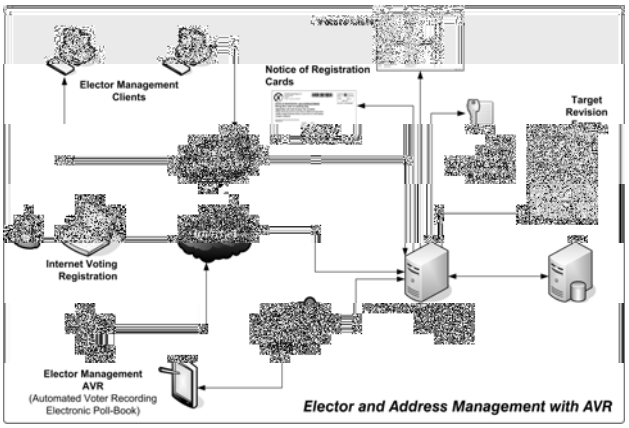


Figure 3: Elector and address management.

3 Data Model

The data model for our automated election services is structured around three databases: *elector management*, *election event*, *security* database. Each of the databases model the real election related entities and their relationships. Electors and their addresses, as well as related administrative data are stored in *elector management* database, together with the voting channel type and elector status (voted, not-voted). The *election event* database contains data related to particular election event such as contests and candidates. This database also stores voting results for a given election event. Finally, the *security* database models electoral organization roles, permissions and retains a log of all activities performed by the users of the system.

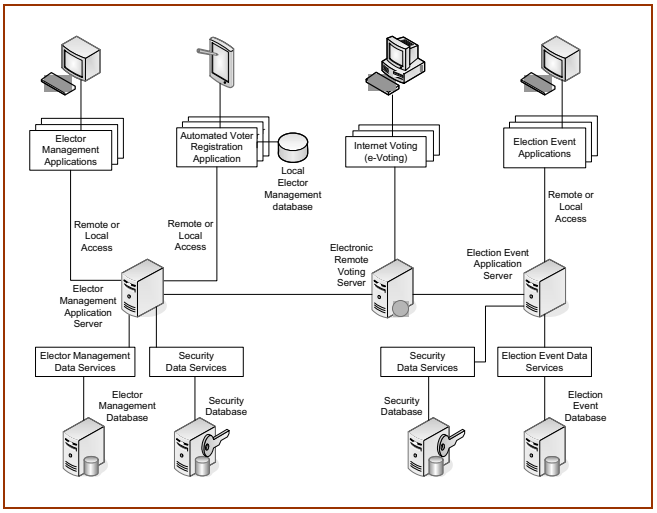


Figure 4: Data model for our automated election services.

The data in the Elector Management database model can be classified into the following categories in relation to an election event and election cycle:

a) Logically detached from election event
b) Logically attached to election event
c) Logically semi-detached from election event

The data in Election Event database has validity only during a particular election event for which they are defined – i.e. list of contest and candidates will change between different election events.

All the tables in our data models can be divided into four categories: *Entity*, *Type*, *Log* and *Mapping* tables. Examples of Entity tables are *Person*, *Poll*, *Candidate*, etc. These tables always use GUIDs as primary keys and contain primary election entities. Examples of Type tables are *LocationType*, *VotingChannelType*, etc. These tables always use integers as primary keys and define election entity or action types as enumeration values expressed in different languages. Examples of Log tables are *VotingLog*, *AdvancedVotingLog*, etc. These tables record all election cycle and election event related activities such as time and place where someone has been voting. Finally, Mapping tables provide support for various levels of relationships between different entities. Examples of these tables are *LocationHandlesPoll*, or *PollUsesBallot*, etc.

From software architecture point of view, both Election Event and Elector Management Application Servers, as guardians of database access and management, implement optimized and concurrency safe data access layers. These software components are not only responsible for direct database access, but also for Object to Relational Mapping (ORM) between database tables and their relationship on one side, and domain objects on the other. This architecture provides robust election specific domain access and clear view toward the election data models.

4 Democracy Suite Software Components

The two core software components of Democracy Suite are Election Event and Elector Management application server. These two server components implement automated election workflow intelligence and communicate with corresponding data models. These application server modules are deployed utilizing encrypted binary transport channels and a variety of client applications and dedicated task-oriented services:

a) Election Event Definition – set of pre-voting modules for defining election events, programming of the voting channels and creation of ballots, either paper of electronic.
b) Results Tally and Reporting – set of post-voting modules for acquisition of election results from the voting channels, manual data entry, results verification, tally and publishing. In addition, auditing of the overall voting process is integrated in this module.
c) Elector Management – responsible for the importing, cleansing, maintenance and real-time tracking and registration of electors. In addition to importing elector data from a variety of data sources, this system creates:
    i. Notice of Registration Cards (NRCs), or invitation to participate (vote) in a given election event.
    ii. Electronic and paper poll-book lists that can be used in combination with the our Automated Voter Recording system and the CF105 electronic poll-book platform,
    iii. Elector Identification Numbers (EINs) used as secure PINs for remote electronic voting (e-Voting), and
    iv. A list of voters and addresses for a subsequent target revision process which should provide a clean and up to date list of electors for the next election event.
d) Remote Electronic Voting – includes a support for Internet voting, which basically includes Registration Server, Electronic Ballot Issuing Server, Internet Voting Server and Electronic Ballots. All these components work in harmony with Election Event and Elector Management subsystems.

5 Automation of Paper Ballot Voting

A majority of the elections in Canada, and also in other parts of the world, remain based on a paper ballot system and in-poll voting. We can expect that this traditional voting channel will be in use for some time as a result of cost, accessibility, and permanent audit record considerations. Therefore, one of the primary goals of our strategy was to automate that process as much as possible using a specialized set of software and hardware solutions.

From a hardware point of view, we have designed an electronic voting box (CF200) in the form of optical ballot tabulator (Figure 5) with integrated audio vote capabilities and variety of communication options.

This device, especially designed for decentralized deployments (for in-person voting), deploys a reliable two-sided high-resolution digital scanning mechanism with on-board advanced image processing algorithms for optical mark recognition. Every ballot scanned is saved and permanently imprinted with the results of the vote determination algorithm. This patented feature provides a fully auditable paper and electronic trail. Also supporting special requirements for people with disabilities, the CF200 deploys audio ballot feature for greater accessibility. Visually impaired and other people with disabilities can use this feature to cast their votes.

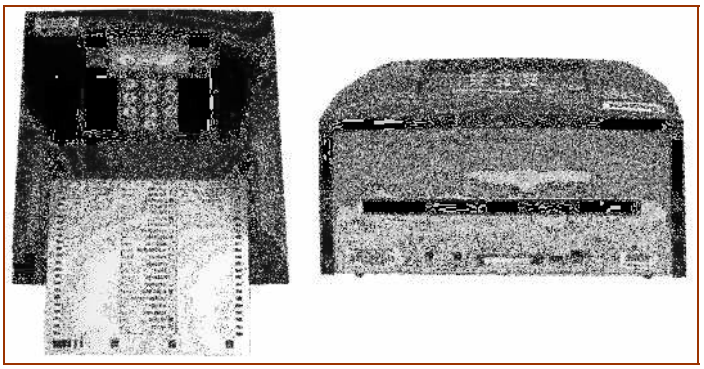


Figure 5: The CF200 electronic voting box in the form of optical poll-level tabulator.

For all central count applications reliable high-speed scanning hardware has been integrated with high-performance and accurate image processing algorithms. Depending on the scanning performance, ballot size and layout requirements, appropriate central count solutions from CF500 series can be selected. The CF500 is the most suited for high-turnout elections with scan rate of 6000 ballots per hour and ballot size of up to A3 format, while the CF520/40 models are designed for mid-turnout elections with scan rate of up to 2500 ballots per hour and ballot size of up to A4.

The image processing module within Democracy Suite leverages the binary nature of the scanned ballot images and provides high speed tabulation utilizing a two-dimensional signal correlation algorithm for tracking form landmarks. Prior to this approach, the optical tabulation platforms used a rudimentary bounding box technique together with a straightforward pixel counting method for detecting form answer fields. Although this technique was extremely fast, it was highly susceptible to printing inconsistencies, scanning noise and image skewing. Furthermore, the decision process for any given voting field (i.e. detection of mark or no mark for a given candidate) employed fixed rotation bounding boxes that did not accommodate for even minor image skews.

In order to speed up processing, the new algorithm uses an iterative search space which converges on the location of the desired ballot marking field by varying the search space extent and resolution until a specified threshold is reached. This use of pattern matching is superior to a simple bounding box technique because it is able to filter noise more effectively as well as account for some variations in skew as the most likely result is used in the analysis of voting boxes. The new technique has been able to successfully detect votes that have been inadvertently cut off during scanning, markers obscured by printing or scan head artefacts, as well as markers that have been tampered with (e.g. written on). In addition, form skew is taken into consideration, allowing the bounding box of the answer area to be rotated appropriately, and thus provide more accurate pixel counts.

Both the compression algorithms used to save ballot images and the file formats are different for the poll level (CF200 series) and central count (CF500 series) tabulators. On the CF200 series tabulators, the images of all scanned ballots are compressed using run length encoding (RLE) and stored as a BMP files. Since the images are binary (black and white), RLE is very efficient in compressing the images up to 15 times. On the CF500 series tabulators, TIFF LZW (Lempel Ziv Welch) is used for image compression to save all scanned ballots. TIFF LZW is the de-facto standard for lossless image storage. LZW is the most popular compression for black and white and grayscale images. This algorithm compresses and decompresses without any information loss, achieving compression ratios up to 5:1.

From a software point of view, Democracy Suite includes several software modules for automation of paper-based voting. Election Event Definition modules include Election Event Designer and Ballot Designer features. While first one is used for collection of contest and candidate names, as well as administrative electoral divisions, the second one creates ballot styles and layouts using predefined ballot templates. This complete set of information is used for creation of binary voting configuration files for programming of voting channels. Another set of software automation tools are used for result tallying and reporting. These modules are responsible for election results acquisition from various voting channels, manual results data entry, results tallying, verification, auditing and reporting. Each voting channel produces the results information file in a common binary format. After importing these result files into the Results Tally and Reporting module, votes cast are stored in a temporary database giving the electoral officers the opportunity to perform results verification before making results public. This verification can be selectively performed either for all contests or just for contests flagged as critical. Finally, in an auditing process using a random algorithm, electoral officers and scrutineers can select ballots for inspection and compare images of scanned ballots with system recordings. Using this approach, a very high level of acceptance is achieved in the overall tabulation validity.

6 Electronic Remote Voting

Electronic Remote Voting (Internet voting) has some unique requirements that differentiate this method from traditional paper-based voting processes. In recognition of these unique requirements, a 5-step process was defined as shown in the following diagrams.

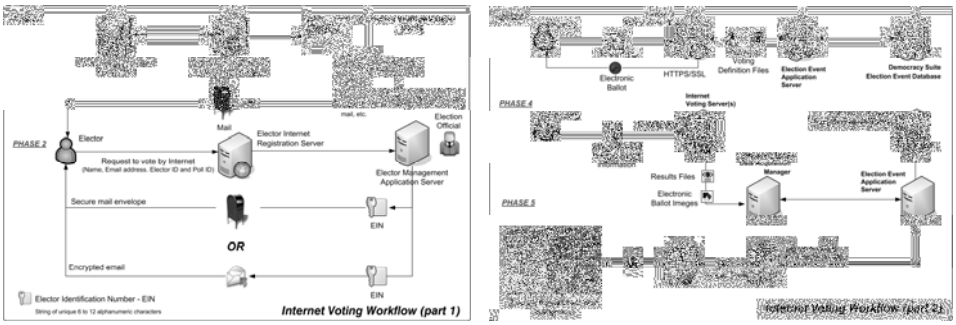


Figure 6: Internet voting five step process.

Phase 1 – Elector Management - This phase is common for any type of election, regardless of the voting method(s) being employed. At the end of the elector management process, the system generates the invitation to vote (NRC) cards to be mailed to eligible voters. Each NRC card contains information about the voter including name and address, unique elector identifier (Elector ID), etc.

Phase 2 – e-Voting Registration - Upon receipt of their NRC cards, voters can choose to vote using a traditional paper ballot at the polling location, or to register to vote using the Internet voting. If an elector chooses to vote via the Internet, they must first register at the designated Internet site (Internet Registration Server). Based on this information, the system generates a unique Election Identification Number (EIN) for that elector. This EIN serves a similar purpose to that of the PIN numbers commonly used in Internet banking. This number is communicated to elector using the secure mail service.

Phase 3 – Electronic Ballot Download - On the Election Day(s), electors who received EIN codes can access the Internet Ballot Issuing Server and proceed with voting by downloading an electronic ballot. Every electronic ballot is generated dynamically by mapping elector information with content in Election Event database. In addition, each ballot contains a randomly generated Ballot Activation Code (BAC), which is embedded into the ballot in the form of 2D barcode matrix. This code ensures that one ballot is issued and cast only once.

Phase 4 – E-Voting – A sample electronic ballot is presented in Figure 7. Electronic ballots can have animated help, configurable marking options (square, oval, circle, arrow, x, check mark, etc.), audio capabilities, magnification features, etc. This is especially important for visually impaired people who can vote using these special features. The voting process itself is identical to marking a paper ballot. After making a selection, the elector presses a Submit button which is followed by a confirmation screen. Depending on configuration settings, this system can prompt an elector to correct his selection if the ballot is blank, overvoted or undervoted. After elector acknowledgement, votes are extracted from the ballot and serialized to the Internet Voting Server over the secure communication link. At this point, the used EIN code is destroyed and the elector voting state is appropriately changed. For each electronic ballot cast, electronic image of the ballot is created. Using this approach, even electronic voting can have auditing trail (images can be printed and used as the paper ballots) and in case of a recount, the electronic voting process does not have to be repeated (generated images can be scanned using optical tabulators together with other paper ballots).

Phase 5 – Results Tally and Reporting - The results processing and reporting phase is the same for all methods of voting, including Internet voting and traditional paper ballot voting. The Internet Voting Server produces results files in the same format as those produced by the paper ballot tabulator devices.

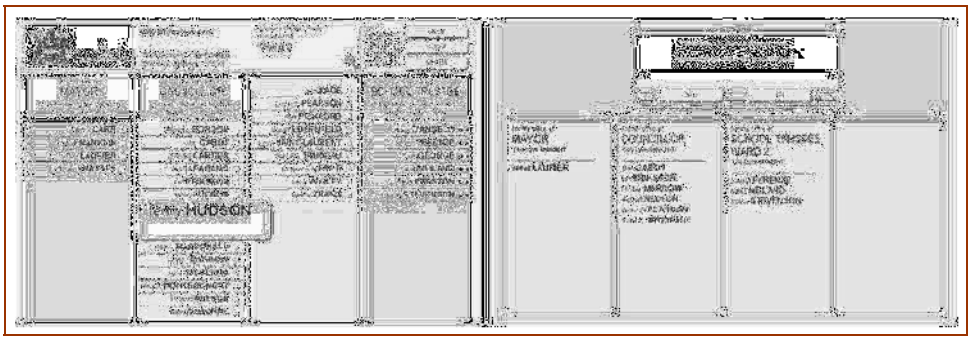


Figure 7: Sample electronic ballot with zooming feature.

7 Reporting

All reports can be divided into the following groups:

a) Election Event Definition reports provide information about the structure of the defined election event, with all of their election entities and their relations.

b) Elector Management reports include all of the information about the list of eligible electors, issued and mailed NRCs, status of electors (list of voters who voted at advanced polls and regular election days), list of issued certificates to vote, list of issued proxies, etc. The system keeps track of all electors who have registered to vote by Internet, along with their voting status.

c) Internet Voting Services status reports provide information about electronic ballots issued, along with the status of the Internet servers and connections, alarms (if any), etc.

d) Election Results Tally and Reporting module produces up-to-date PDF/Excel/XML reports in addition to the live web streaming reports, based on rich-content data representation (maps, tickers, charts, grids). Live web reports are fully customizable in terms of content and layout (Figure 8, left), providing interactive and dynamic results representation format at the election night (Figure 8, right).

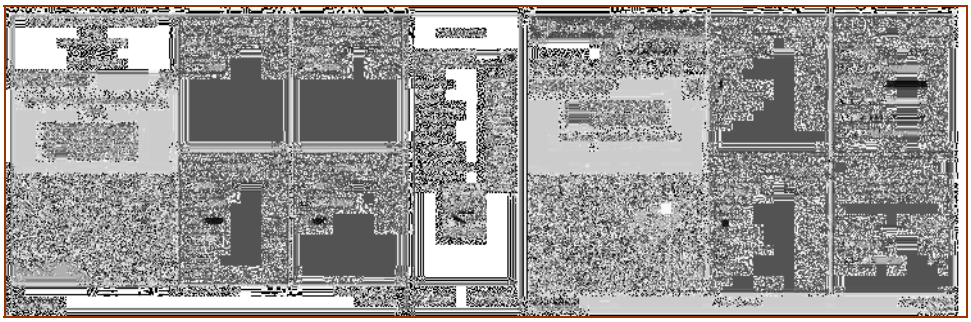


Figure 8: Live web streaming election results presentations.

8 Conclusions

In this paper we have presented automated election workflow based on Democracy Suite line of software and hardware products. Democracy Suite has a range of features to handle contemporary election issues. Computer technologies are utilized in order to provide ballots in a greater variety of formats to reach a larger percentage of electors. High migration is handled more effectively with database tools for elector list management. Automation is introduced into the poll to provide assistance to electors and also to support more complicated ballot styles. All security concerns for both internet ballots and election management have been addressed to ensure system integrity. Full attention is granted to election event and election cycle entities to minimize the required time required to stage an election. Our current work includes additional system improvements for making the Democracy Suite fully compliant with [FEC05] specifications.

Literature

[EML05] OASIS: EML (Election Markup Language) Schema Descriptions – Version 4.0., 2005.

[EA05] Election Act, Canadian Government, 2005.

[FEC02] Voting Systems Standards, Federal Election Commission, USA, 2002.

[FEC05] Voluntary Voting System Guidelines, Federal Election Commission, USA, 2005.

[HAVA02] Help America Vote Act, Federal Election Commission, USA, 2002.

Session 6: Observing E-Voting

A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament

João Falcão e Cunha, Mário Jorge Leitão, João Pascoal Faria,
Miguel Pimenta Monteiro, Maria Antónia Carravilla

Faculdade de Engenharia da Universidade do Porto
Rua Dr. Roberto Frias
4200-465 Porto, Portugal
{jfcunha | mleitao | jpf | apm | mac}@fe.up.pt

Abstract: In the 2005 Portuguese Parliament General Elections there were non-valid experiments of e-voting at five voting places and also through the Internet. *Faculdade de Engenharia da Universidade do Porto* audited such experiments. Relevant *security*, *transparency*, *usability* and *accessibility* evaluation criteria and sub-criteria were defined, and an auditing procedure based on AHP was established. This paper shortly presents the methodology used, the four e-voting systems and the main results of the overall experiment. The systems could be used successfully and were extremely popular with voters. However, more information to the citizens and to the officials involved in the e-voting process would be required for a valid election. The systems also need to be improved, for instance, to make sure that the number of votes electronically cast is the same as the number of voters that were validated and actually registered to vote at any particular site on the Election Day.

1 Introduction

1.1 Context

During the previous elections for the European Parliament, in 2004-06-13, and for the general elections for the Portuguese Parliament, in 2005-02-20, the government and the parliament agreed to carry out a set of experiments on electronic voting.

For the European Parliament elections there were 9 boroughs involved, geographically and socially dispersed, some in large towns with highly educated voters, and some in small villages with pensioners having little contact with technology. From a total 52 000 electors who cast a valid vote, 9 359 voted electronically (18%) [FE04].

For the elections for the Portuguese Parliament the selected boroughs corresponded to the 5 sites where the President of the Republic and the leaders of the political parties represented at the parliament voted. As Portuguese citizens registered to vote abroad could do it by postal vote (remote vote allowed), it was also decided to set up an Internet voting system. In all cases e-voting was voluntary and not valid, and who cast their vote traditionally was invited to also vote electronically. From a total of 26 515 electors who cast a valid paper vote, 8 824 also voted electronically (33%). From a total of 148 159 electors outside Portugal who were registered to vote by mail, 36 391 voted by mail (25%) and 4 367 voted through the Internet (12% of mailed votes) [Pi05]. After voting, each citizen was personally interviewed by an independent organization in order to collect an opinion about the experience (see below). In the Internet case, the voter could fill in a questionnaire for the same purpose.

Several public and private organizations were involved, but UMIC www.umic.pt, a special government unit with the overall mission of promoting innovation, was in charge of coordinating the project. CNE www.cne.pt and STAPE www.stape.pt, the public entities that oversee and manage general elections in Portugal were also deeply involved. CNPD www.cnpd.pt, a parliament controlled but autonomous unit that oversees the use of information and databases with personal information was also asked to audit and certify procedures. INDRA, MULTICERT, NOVABASE and UNISYS provided the e-voting systems (EVS) for the experiment. MULTICERT, under the guidance of UMIC and CNPD also had the overall responsibility of putting together a digital electoral register for all voters involved in the experiment, and to deploy such system during Election Day at all sites.

The experiments were very successful from the point of view of the voting citizens [OS05]. According to the exit interviews, 99.2% of the citizens that voted electronically enjoyed the experience and 98.1% said they would vote electronically in future elections; 80.5% trust the security of the EVS; 84.5% of the voters that had a paper trail option in the EVS used, consider important that the vote had been printed in paper and automatically inserted into a box; 86.3% consider that if such systems allow people to vote from other places then more people would vote. For people voting through the Internet the results were similar: 99.2% enjoyed the experience and 98.3% said they would vote in this way in future elections; 57.8% trusts the security of the EVS, 7.9% thinks it is not secure, and 34.3% do not know or do not answer the question. Regarding the security of Internet voting, only 1.7% thought it is totally secure against attacks from hackers, while 54.3% do not know or do not answer [UM05].

In order to guarantee the transparency of the process, Universities were invited to make proposals for auditing the process. In the case of the elections for the European Parliament five Universities were involved. Given the fact that it was difficult to manage so many auditors, UMIC agreed that for the Portuguese Parliament's elections there would be a call for tenders regarding the auditing process. *Faculdade de Engenharia da Universidade do Porto* (FEUP) was selected as the main auditor, on the basis of the quality of proposed work, experience and qualifications of the auditing team, price and schedule of work.

1.2 The voting experiments

Five e-voting sites were set-up requiring voters to go to the voting place. One of these sites had six e-voting places allowing the citizens to vote outside their traditionally appointed paper voting place. An Internet system was also deployed to allow e-voting from Portuguese voters registered as residing abroad.

Figure 1 describes the general set-up for the experiments during the Portuguese Parliament's elections.

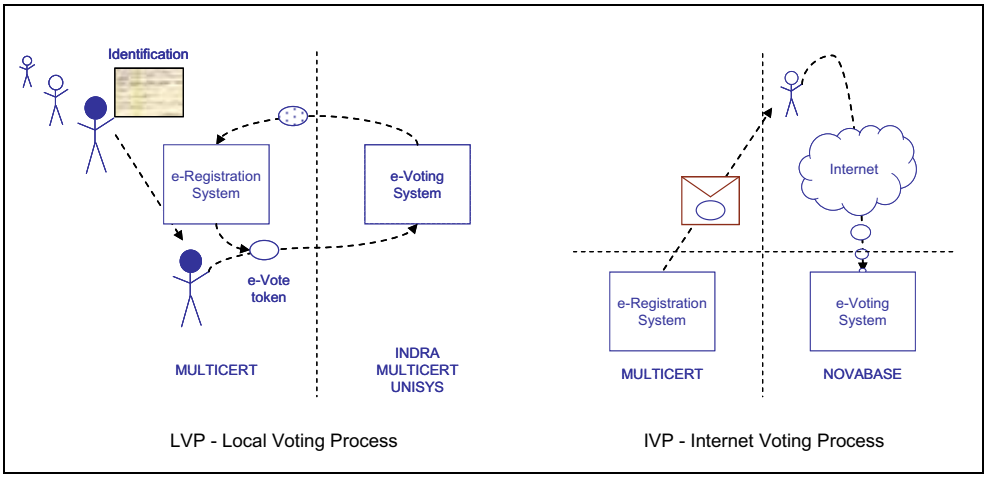


Figure 1: LVP: a citizen with a proper identification gets a token at e-Registration and then can vote. INDRA had one token for each voter, but in the other systems the token is reused after a new permission is granted. Number of voters and votes are counted both at e-Registration and at the e-Voting system. IVP: a citizen that is registered to vote gets an envelope by mail with a token (username and password). He may then log into the e-voting system.

2 The Auditing Methodology

The objective of the auditing methodology was to produce a thorough report on each EVS and to apply scores for each one on the criterion defined by UMIC: Security, Usability, Transparency and Accessibility.

Due to the characteristics of the process, there were 14 auditors involved. This is a large number, and there is a strong need to obtain scores for the EVS that consistently reflect the views of the group as a whole, and not just 14 different views. In order to simplify the assessment, the 4 criteria were decomposed into several sub-criteria. The Analytical Hierarchy Process (AHP) ([Sa80], [Sa87]), which is based on the comparison of the importance of each pair of sub-criteria, was the tool used to obtain weights of each sub-criterion under each criterion, aggregating the views of all the auditors.

2.1 Team composition

The auditing team members' had deep technical and management expertise. They had doctorates in Computer Science, Telecommunications, Security and Information Systems. There was 1 overall coordinator, 4 auditing teams with 3 or 4 elements each (as there were 4 different EVS), and 1 team with 2 elements, both with doctorates in Operations Research, that acted as facilitators during the whole process.

2.2 Phases of the process

The methodology followed by FEUP had three phases, corresponding to the periods before, during and after the Election Day.

Before the Election Day the team met several times in order to make decisions on the criteria and sub-criteria, on the assignment of the auditing team members to the e-voting systems (EVS) and voting periods, and on the set of questions and requests for information to send to each company.

At the Election Day, in order to make possible a comparative classification of systems for the same criteria and sub-criteria, each auditor visited at least two different EVS. There was always an auditor at each voting site, observing the opening moment, the voting process and the final closure, including the vote counting and the communication of results to the counting centre. There was also an auditor at the counting centre.

After the Election Day the auditing team had also at least one meeting with each company, in order to ask further questions that did arise during the audit. With all the information on-hand the auditing team had a long final meeting, facilitated by the Operations Research team, to discuss the scores given for each EVS on each sub-criterion. Taking into account all information, a report on each EVS was produced and sent to UMIC and then to each company.

The procedure for auditing the Internet EVS was adapted from this one as there was not an Election Day but an election period of several weeks. Such votes could only be counted after the postal votes were counted, two weeks after the actual Election Day.

2.3 The evaluation criteria and sub-criteria

The evaluation criteria (Security, Usability, Transparency and Accessibility) were defined a priori by UMIC. During several meetings that took place before the Election Day, the auditing team agreed on the sub-criteria under each one of the evaluation criteria (see Figure 2), based on [Ne93], [BH04], [Ca04], [Me00], [Mo01] and [Pi04]. These meetings were very important for the auditors to discuss and get a consensus on the meaning of each sub-criterion. As, during the Election Day, the teams could not meet and discuss the evaluation criteria it was necessary to promote a discussion on the criteria and sub-criteria with all the auditors, in order to obtain homogeneous evaluations.

SECURITY (S)		100,0%
S1	Audit-ability	10,3%
S2	Operator authentication	4,4%
S3	Certify-ability	9,0%
S4	Reliability	9,8%
S5	Detect-ability	4,6%
S6	Availability of system	5,4%
S7	Immunity to attack	8,1%
S8	Integrity of votes	14,4%
S9	Invulnerability	9,3%
S10	Traceability	3,8%
S11	Recoverability	5,3%
S12	Fault tolerance	4,6%
S13	Isolation	2,6%
S14	Security of communications	8,3%

TRANSPARENCY (T)		100,0%
T1	Anonymity	11,3%
T2	Atomicity	7,0%
T3	Authenticity	11,5%
T4	Trust	6,2%
T5	Technical documentation	2,2%
T6	Integrity of personal	2,8%
T7	Integrity of system	6,0%
T8	Non-coercion-ability	10,5%
T9	Precision of system	7,6%
T10	Privacy	7,6%
T11	Singularity (non reuse)	10,7%
T12	Transparency of process	3,5%
T13	Transparency of system	3,9%
T14	Verifiability	6,5%
T15	Separation of roles	2,9%

USABILITY (U)		100,0%
U1	Easiness of use	38,4%
U2	Speed of use	10,1%
U3	Clarity of language in interface	23,4%
U4	Localisation of interface	11,1%
U5	Emotional satisfaction	17,0%

ACESSIBILITY (A)		100,0%
A1	Convenience	14,4%
A2	Right to vote	47,0%
A3	Documentation for the elector	7,6%
A4	Flexibility	11,9%
A5	Mobility	19,1%

Figure 2: Criteria and sub-criteria for auditing, with relative weights [FE05].

As an example, the sub-criterion "Availability of the System" was described as "During the voting period, the EVS must always be available for all the actors, particularly the voters, in order for the process to run normally". Again as an example, a score of 1 would be given to an EVS that could work during the whole election day, if nothing wrong happened, a 3 if the system would for instance include a battery, that would allow it to work for at least 30 minutes without external power supply, and a 5 if the system would work, based also on batteries, during the whole election day. Such concrete guidelines are not always possible to define, but are desirable for consistent evaluations.

During those meetings it was also necessary to obtain the weight of the sub-criteria under each criterion. The tool used to obtain these weights is called Analytical Hierarchy Process (AHP) and is based on the comparison of each pair of sub-criteria by their relative importance. Every team-member had to fill-up a matrix (see Figure 2) comparing each pair of sub-criteria under each criterion. A 1 means the sub-criteria are equally important, a 9 means, for instance, that "Right to vote" is extremely more important than "Flexibility". The pairwise comparison matrix for each criterion was obtained by calculating the average of the answers of the team members. The AHP methodology was then applied to each criteria matrix leading to a balance of the sub-criteria under each one of the 4 criteria.

Accessibility	A1 Convenience	A2 Right to vote	A3 Documentation for the elector	A4 Flexibility	A5 Mobility
A1 Convenience	1	1/7	6	9	1/6
A2 Right to vote	7	1	9	9	8
A3 Documentation for the elector	1/6	1/9	1	1/6	1/8
A4 Flexibility	1/9	1/9	6	1	1/7
A5 Mobility	6	1/8	8	7	1

Figure 3: Matrix for the pairwise comparison of the sub-criteria of the Accessibility criterion.

After the Election Day, the auditing teams met to evaluate each EVS on each sub-criterion. This evaluation was given simultaneously to all the EVS after a general discussion and an agreement of the auditors involved. The score of each EVS under each criterion was obtained by calculating the internal product of scores with the weights of the sub-criteria under each one of the 4 criteria. The final result is shown in Figure 4.

	UNISYS	INDRA	MULTICERT	NOVABASE
Security	4,2	4,1	2,6	3,6
Transparency	4,2	4,3	3,2	3,0
Usability	4,2	3,9	2,7	3,8
Acessibility	3,7	3,3	3,5	3,6

Figure 4: Final evaluation under the 4 criteria of the 4 EVS (scale 1-5).

3 The e-Voting Systems and Associated Processes

The e-voting experiments involved hardware and software from 4 enterprises: MULTICERT, UNISYS/ESS, INDRA and NOVABASE. As mentioned in the introduction, MULTICERT developed the elector registration system used in all experiements and NOVABASE developed the Internet voting system. There were two kinds of presential voting systems: The *local voting* systems required that voters would go to their traditional voting place. This was the only location where they could cast their electronic vote. In the *local voting with mobility* system the voter could choose one from several places where to vote, all located in the same borough. All systems are shortly presented in the next sections. For further details see [FE05].

3.1 INDRA – Local Voting

The system proposed by INDRA is named Point&Vote. It consists of special purpose equipment based on a standard PC platform equipped with a touch screen with side view protection, a smart card reader and an internal printer for reports. The unit is portable and must be placed on top of a table. Two alternative versions were available, one with headphones and mouse for physically impaired voters, and another with a printer, where votes could be seen for a few seconds by the voter, but could not be removed from the collecting basket. This version was intended for evaluation of the need of a paper trail.

In order to vote using the INDRA system, each citizen receives a smartcard. This token is required to enable the use of the actual voting machine were votes are cast (and counted at the end of the Election Day). After being used the smartcard is returned to the e-registration and is not used again at the current election.

At the end of the voting period, each Point&Vote machine is closed with the operator (supervisor) smartcard and password, thus disabling any further voting action. Results from each machine can now be locally printed and transmitted subsequently over the internal modem via a secure communications link to a computer of the Central Election Authority.

3.2 UNISYS/ESS – Local Voting

The system proposed by Unisys and manufactured by Election Systems and Software (ESS) was the iVotronic. It can be generally characterised as a touch screen voting unit, portable and easily configurable (height and orientation), with good privacy protection. These features, plus an optional audio interface, allow good support to visually impaired and wheelchair locomoting voters.

The PEB (Personal Electronic Ballot) is the token that gives access to one vote in the iVotronic machine, prevents overvoting, and notifies the voter in the case of an incomplete operation (such as removing the PEB from the iVotronic unit before pressing the physical VOTE button). It's a sealed unit communicating within a very short range through a proprietary infrared technology and protocol that was designed to prevent communication with standard IrDA transceivers. After each use the PEB must be regenerated in a specific machine with the proper infrared interface.

Some special operations can be performed using a different supervisor PEB requiring explicit password validation. If validated, operations such as opening a voting session (zeroing the counters), closing the voting session, or casting or eliminating incomplete votes (when the voter didn't press the VOTE button), are allowed and logged. During the voting session results are accumulated internally and redundantly recorded (in 3 different flash memory units). All operations, including the supervisor actions, are also timed and logged.

At the end of the session the voting units must be closed and its accumulated results transferred and added to the supervisor PEB memory, allowing several units to be combined in a single one. This PEB is then read in another machine, which also can combine several results. This machine can now print the results (totals and partials) and transmit them to a computer of the Central Election Authority using a modem and a phone line.

3.3 MULTICERT – Local Voting with Mobility

Differently from the previous systems, the MULTICERT voting system allowed citizens to vote electronically in a place different from their traditional one, within the same borough. In the future, the goal of the system is to allow citizens to vote in any other borough.

This was achieved by a distributed e-registration system, based on a central database that stored information about what electors had already voted, and was remotely accessed by client applications located in each place.

Another distinguishing feature of this system was the existence of an electronic ballot box system (EBBS) that actually stored the electronic ballots, separated from the electronic voting units where the electronic ballots were filled in. Small i-button devices were used to carry authorizations (similar to empty ballots) from the EBBS to the electronic voting units, and carry back filled in ballots to the EBBS.

Besides a touch screen, each electronic voting unit had a small printer to print and store paper ballots corresponding to the electronic ballots, with the purpose of enabling non-electronic ballot recounting and improving the confidence on the process. The elector could check by visual inspection that the printed ballot corresponded to his electronic ballot.

Special operations could be done in the EBBS using supervisor i-buttons, namely start a voting session (zeroing the counters), close the voting session, and subsequently view on screen, print and export the results. The results were not transmitted electronically.

3.4 NOVABASE – Internet

The Internet voting system was aimed at all the citizens registered to vote outside of Portugal using postal vote. Two separate mailings were sent to voters abroad: the one containing the valid ballots and another one with the information and keys to allow the vote using the Internet system. The Internet voting process (i-voting), had the following steps:

1. Using a database of electors the system generates individual credentials for each one, a unique code of a username and a password.

2. The electors' information is registered together with the credential in the Active Directory of the central system.

3. The credentials are posted to the electors abroad by mail. The message does not include the elector number, to prevent other people to vote.

4. Pairs of encryption keys are generated. The public key is send to Novabase to be stored in the Database. The private key is divided into 7 parts, one for each political party represented. Votes can only be read with these 7 keys.

5. The vote process is open, allowing browsers to access the server. In the experiment this server was located at the headquarters of Novabase.

6. The elector receives the credentials. He/She can use any computer with a browser, able to accept some JavaScript and cookies, to access the web page www.votoelectronico.pt. He/She has to introduce the elector number and the credential. If all is correct, he/she can then proceed to vote.

7. The confirmed vote is registered in a database table, using two key encryption. The public key is used to encrypt. During the same transaction it is stored that the citizen has voted in the credentials table and in the Active Directory. Afterwards the elector is informed that the vote has been confirmed.

8. At closure of the election the information in the Active Directory is printed and sent to CNE. The Active Directory is erased in the presence of CNPD. A copy of the database is stored and sealed in a CD with a MD5 seal, kept by UMIC.

9. Counting of the votes is done with a special application. As the votes are encrypted it is required to bring together the 7 keys to produce the final result.

The system uses traditional client server architecture. From a logical point of view there is one Web site and clients over the Internet. The Web site is in fact divided in two parts: an http information site and an https secure one, with the forms and vote registration.

4 Conclusions

It is widely accepted that there is very high satisfaction and trust with the current paper based electoral process in Portugal. Most of the citizens cannot evaluate the security or transparency of the computing and communication systems to be eventually used in elections. Certification and audits are therefore required to provide a wide socially recognised guarantee of security and transparency for the new systems and processes.

The audit identified many advantages and problems of the several EVS. One of the problems observed has to do with the inconsistencies in the final number of counted electronic votes. In each voting site there were a number of total electronic votes Nv (counted by the EVS) and a total number of citizens Cv that were given tokens to vote (counted by the e-Registration system). The three situations below occurred. This could be a problem of the EVS, of the procedures people used, or both:

- Nv > Cv. At least one citizen voted twice. It could have happened that one citizen was given more than one chance to vote (e.g.; claimed token was faulty).
- Nv < Cv. At least one citizen did not vote. It could have happened that one citizen actually did not vote at the EVS (not a problem, if voluntary).
- Nv = Cv. All was fine, or pairs of the above happened at the same EVS.

All systems, except the Internet one, suffered from this problem. This can be a major problem facing the adoption of e-voting, and illustrates the need for improved systems and improved voting processes. Improved systems can make the voting process more secure and transparent, as well as more usable and accessible. Improved information to the citizens and to the officials running the election, are key requirements for maintaining trust and satisfaction with the democratic election processes.

The audit method presented did not produce a final ranking of systems. This would require that relative importance would be given to the 4 criteria. Acceptable minimum levels of performance on each criteria (or subcriteria) could have been defined. For instance, one may argue that EVS security level must be over a certain level in order to be acceptable to be used. Both of these decisions, on relative importance of criteria and minimum performance levels, must also involve political involvement.

An improved audit method could include a comparison of EVS with the traditional paper voting system, on the same criteria. Weak and strong points of each type of system could be compared under the same sub-criteria, if making sense.

Acknowledgments

The authors would like to acknowledge the work and contributions of Gabriel David, J. Correia Lopes, A. Carvalho Brito, J. Magalhães Cruz, Sérgio R. Cunha, R. Moreira Vidal, Henriqueta Nóvoa, J. Vila Verde, Miguel Gonçalves, L. Miguel Silva, and J. Fernando Oliveira. The auditing process benefited from contributions from Diogo Vasconcelos, Sara Piteira and João Vasconcelos, from UMIC, and from Fernando Silva, from CNPD. The authors would like to state their appreciation for the very professional attitudes of officials from CNE and STAPE, and from the representatives of all the enterprises that were directly involved in the experiments.

References

[BH04] B. Bederson, P. Herrnson: «Expert Review Plan of Voting Machines», Research Report, HCI Lab & Centre for American Politics and Citizenship, U. Maryland, USA, 2004.

[Bu04] T. M. Buchsbaum: «E-Voting: International Developments and Lessons Learnt», in [PK04], p. 31-41.

[Ca04] Jean Camp, Allan Friedman, Warigia Bowman (ed.): «Electronic Voting Best Practices - A Summary», Voting, Vote Capture & Vote Counting Symposium, Kennedy School of Government, Harvard University, 2004-06, 23 p.

[FE04] (in Portuguese) J. Falcão e Cunha (ed.): «Relatório Final de Auditoria – Eleições para o Parlamento Europeu de 2004-06-13» (Final audit report of the Portuguese electronic elections experiment for the European Parliament); 2004-08-04, FEUP, Portugal, 28 p.

[FE05] (in Portuguese) J. Falcão e Cunha (ed.): «Relatório Final de Auditoria – Eleições Legislativas de 2005-02-20» (Final audit report of the electronic elections experiment for the Portuguese Parliament); 2005-04-21, FEUP, Portugal, 78 p.

[Me00] Rebecca Mercuri «Generic Security Assessment Questions» (www.notablesoftware.com).

[Mo01] (in Portuguese) A. Monteiro, N. Soares, R. M. Oliveira, P. Antunes: «Sistemas Electrónicos de Votação» (Research Report supervised by P. Antunes, DI-FCUL TR–01–9), 2001, Dep. Informática, FCUL, Campo Grande, 1700 Lisboa, Portugal.

[Ne93] Peter G. Neumann: «Security Criteria for Electronic Voting», 16th National Computer Security Conf. Baltimore, Maryland, 1993.09.20-23.

[OS05] (in Portuguese) OSIC – Observatório da Sociedade da Informação e Conhecimento «Voto Electrónico - 2.ª Experiência Piloto de Voto Electrónico Presencial, Resultados Eleições Legislativas de 2005-02-20», 2005-03, 22 p.

[Pi04] (in Portuguese) R. R. Pinto, F. Simões, P. Antunes: «Estudo dos Requisitos para um Sistema de Votação Electrónica» (Research Report supervised by P. Antunes, DI-FCUL TR–04–2), 2004, Dep. Informática, FCUL, Campo Grande, 1700 Lisboa, Portugal.

[Pi05] (in Portuguese) S. R Piteira: «Projecto Voto Electrónico», Voto Electrónico e Defesa da Privacidade Workshop (Electronic Voting and Privacy Protection Workshop), CNPD, Assembleia da República, Lisboa, 2006-12-07, 21 p.

[PK04] A. Prosser, R. Krimmer (Eds.): «Electronic Voting in Europe – Technology, Law, Politics and Society», Lecture Notes in Informatics, GI-Edition, 2005.04.23, 182 p.

[Sa80] T. L. Saaty: «The Analytic Hierarchy Process». McGraw-Hill, New York, 1980.

[Sa87] T. L. Saaty: «The Analytic Hierarchy Process: what it is and how it is used», Mathematical Modelling, 9, 1987.

[UM05] (in Portuguese) «Voto Electrónico - 1.ª Experiência Piloto de Voto Electrónico Não Presencial, Resultados - Eleições Legislativas de 2005-02-20», UMIC, 2005-03.

Voting in Uncontrolled Environment and the Secrecy of the Vote

Kåre Vollan[1]

Quality AS
P.O. Box 5153 Majorstua
NO-0302 Oslo, Norway
kvollan@online.no

Abstract: Voting in uncontrolled environment either by post or by the Internet is about to be made generally available in many countries. The main purpose is to increase participation at times when the voter turnout is generally decreasing. Electronic voting both in or outside controlled environment offers advantages in producing fast and reliable results and long term cost savings in the conduct of elections.

A number of problems relating to security, reliability and general trust can be solved by Internet voting, once an infrastructure for voter identification is in place. However, neither postal votes nor Internet votes can guarantee that the vote is cast in secrecy without intimidation or pressure. Even without the most serious violations to a free vote, the pattern of voting will change and the concept of voting being a strictly personal and secret act is likely to be weakened over time.

There are few reasons to doubt that the introduction of voting by Internet once generally available will have the same success in terms of usage as other Internet services such as bank transactions, tax returns etc. Once being implemented in a user friendly and reliable manner the electronic interface may within foreseeable future become the major voting channel.

This paper does not discuss in depth the legal issues related to whether uncontrolled voting meets international commitments regarding a secret vote. The focus is to what extent the most likely change of voting pattern from a public to a more private, but less secret event, is a positive development. It concludes that the problematic issues which can be raised are fundamental and the long term damage to the perception of a personal and secret vote should be discussed by governments and inter-government organisations. Alternatives such as electronic voting in controlled environment prior to election day may, to a large extent, serve the same purpose without showing the negative side effects of voting outside of controlled environment.

---

[1] The author is a consultant on electoral issues providing advice mostly in post conflict countries and in countries in transfer to democracy. He has also headed a number of international election observation missions and he is a registered IT quality auditor (IRCA).

1 Introduction

1.1 Trends in Voting Methods and Voting Behaviour

The international trend of decreased turnout in elections has led a number of countries to offer possibilities of voting outside of polling stations on election day. The main class of alternatives is variants of early voting (voting before election day) either conducted in controlled environment where the voter has to meet in person and election officials will check that the vote is cast in person and in secrecy or cast in uncontrolled environment by a postal vote or a vote by Internet. In addition voting may be offered to bedridden people by use of mobile teams on or before election day and remote voting may be available even on election day.

Increasing voter participation is clearly the main reason used to offer early voting in various forms, but other reasons will also be discussed below. Early voting in controlled environment is common for example in Scandinavia. In Norway around 20% of all votes cast in the last elections have been early votes [NO00]. Postal votes were first introduced to accommodate groups which would otherwise be disenfranchised such as voters travelling or living abroad or voters with disabilities making it difficult to come to a polling station. However, postal voting has in some countries such as Switzerland, Great Britain and Spain been offered to voters in general. In the general elections in 2005 in the UK the share of voters requesting a postal ballot was 12.1% up from 8.3% during the European Parliament and local elections in 2004 [UK01].

Voting by Internet has been offered in some countries such as Switzerland (in some cantons) and Estonia. In November 2005 23% of all votes cast in the municipalities with the possibilities for Internet voting in Geneva used that possibility. During the 2005 local elections in Estonia less than 2% of those voting cast an Internet vote [NO00].

A number of countries are assessing the possibilities for introducing voting by Internet. The main concern has been the reliable voter identification together with the secure technical implementation of such systems. Public systems for electronic signatures[2], which will help solving some of the security issues with Internet voting, are being introduced. If such public systems are regarded sufficiently secure for bank transactions and public services in general at least the highest security level offered for such services would suffice even for voting. Once the security requirements have been met it is likely that Internet voting will be proposed in a number of countries in the years to come. Once introduced it may show the same effect as other Internet based services and a major share of the votes cast may be Internet votes but whether Internet voting will increase the total turnout or just replace other means of voting remains to be seen.

[2] PKI – Public Key Infrastructure.

The Council of Europe has assessed electronic voting in uncontrolled environment against international obligations and commitments in the Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting [CE03]. The recommendation states:

> "Bearing in mind that the right to vote is one of the primary foundations of democracy, and that, consequently, e-voting system procedures shall comply with the principles of democratic elections and referendums;
>
> Recognising that as new information and communication technologies are increasingly being used in day-to-day life, member states need to take account of these developments in their democratic practice;
>
> Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;
>
> Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:
>
> – enabling voters to cast their votes from a place other than the polling station in their voting district; …"

When discussing the international commitments the recommendation says:

> "IV. Secret suffrage
>
> 16. E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.
>
> 17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.
>
> 18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.
>
> 19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote. "

The secrecy of the vote is only discussed in the technical context in the paper: The system need to be designed in such a way that individual votes cannot be identified once the result is established. The conclusion has also been shared by the Venice Commission [CE03]:

> "1. In conclusion, remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either non-supervised postal voting or electronic voting."

The fact that the voter may not be alone when casting the vote is much less prominent in the documents from the Council of Europe. This is a fundamental feature of both Internet and postal voting. Even if the vote once cast cannot be traced to the voter, the secrecy of the vote cannot be guaranteed. So far international observer missions and organisations have concentrated on security issues and much less on problems related to votes cast in groups with possibilities for undue pressure and even intimidation.

There is not full international agreement to whether uncontrolled voting complies with the requirements for secret votes. A number of countries have decided to be restrictive in offering such possibilities and if the do it is only offered to groups of voters who would clearly otherwise be disenfranchised. Other countries have decided to open such possibilities for all voters and their view is that the voting still complies with international standards as long as a controlled alternative is offered. This paper will not discuss the legal aspect of the question in full depth even though the international commitments are listed below. The subject for this paper is rather to what extent the development towards more uncontrolled voting is a positive development. By offering voting in uncontrolled environment to voters in general the concept of elections is being changed without a thorough discussion of the most likely end result: Voting may not be a secret act any more but may be carried out by voters sitting together, in families, in groups of young people, in community centres etc. This may open the vote for intimidation, trade with votes etc. But even if the most serious violations will be limited the effect over time may be that the concept of a personal, secret vote is weakened.

1.2 Types of Voting

Direct elections to national and local representative bodies have traditionally been conducted in polling stations during one or few election days. Polling station staff ensures that the vote is cast in person and in secrecy free from intimidation and pressure of any kind. Under various conditions many countries have allowed for early voting, postal voting and recently voting over the Internet.

It is common to differentiate between the following types of voting:

a. Voting in controlled environment, means any voting where election staff overlook the process of casting the ballot. This may happen in a polling station on election day or in a particular site for early voting.

b. Voting in uncontrolled environment either as a postal vote or by the Internet. In these cases it is up to the voter to secure the physical environment under which the ballot is cast.

The ballot may be a paper ballot or an electronic ballot. In addition the vote is conducted in phases:

a. The phase prior to elections day, the early voting
b. The election day(s) voting.

Voting types may be illustrated by the following matrix [NO01]:

	Controlled		**Uncontrolled**	
	Early voting	**Election day voting**	**Early voting**	**Election day voting**
Paper	At defined sites with regular paper ballots	Traditional polling stations with paper ballots	Postal votes	Postal votes
eVoting	Voting machines at defined sites	Voting machines in polling stations	Internet Voting	Internet Voting

Figure 2: Overview of types of voting

2 International Commitments Related to the Types of Voting

According to broadly accepted standards election should be *universal, free, fair, secret* and *transparent* [OD04].

A *free* vote means that the ballot is cast in person free from intimidation and undue pressure. *Universal* means that every citizen who has reached a certain age and fulfil accepted criteria can cast a vote. *Secret* would mean that the person can rest assure that the vote will not and can not be disclosed to anybody. This does not prevent a voter from volunteer his or her choice but it should not be possible to verify the information given by the voter. *Fair* means that candidates run under the same conditions and their supporters have the same fair chance to take informed decisions and cast the vote. The requirement of being fair would also imply all votes should be counted correctly, the tabulation should be correct and the process protected against fraud and mistakes. The best guarantee against fraud and mistakes when using traditional technology is *transparency*. This is assured by the possibility for representatives of all stakeholders to witness every step of the process, from the voter enter the polling station to the protocol is drawn up and the results are tabulated. The only exception is when the voters are making his or her personal secret choice.

The different types of voting will score differently for each of the commitments, which the table below indicates:

	Controlled		**Uncontrolled**	
Commitment	**Paper**	**Electronic**	**Paper**	**Electronic**
universal	Medium	Medium	High*	Very High*
free	Very High	Very High	Very Low	Low
fair	Very High (-)	Very High (+)	Low	High
secret	Very High	Very High	Very Low	Very Low
transparent	Very High	Low (-)	Low	Low (-)

* The high scores are in particular set for situations where uncontrolled voting comes in addition to voting in the polling station, but may eventually deserve a high score even if uncontrolled voting were the only option.

Figure 2: An indication of how controlled and uncontrolled voting meets international criteria for elections.

The table is meant as an indication only. The rating clearly depends on how each type of voting is implemented. It is possible to conduct paper voting in a polling station without any transparency and one may improve transparency for electronic voting in polling stations by printing a paper which can serve as an audit trail. The rating should reflect situations where regular procedures are applied by an election management body (EMB; that be a ministry, an independent election commission or any other body charged with the overall election administration responsibility) in good faith in order of conducting correct elections.

Voting outside controlled environment is being used mainly to strengthen the *universal* quality of the vote. By requiring voters to meet in person in a polling station on election day, bedridden people, people with disabilities, people travelling etc may be disenfranchised. In addition some voters may just decide to go to the polling station, but they may choose to vote by mail or by Internet if given the chance.

The freedom and secrecy can clearly best be guaranteed when the vote is cast in controlled environment. This is the only place where officials can make sure that the vote is cast without undue influence of any kind.

A *fair* election would on polling day mean that the process works as intended. Even in traditional democracies the controls and checks have not always been implemented in such a way that deliberate attempts to cheat could be resisted. Often the identity of the voter is not checked, voting material may not be secured and the rules for secret voting may have been rather relaxed even in polling stations.

On the other hand in controlled environment the possibilities for preventing impersonation, intimidation and group pressure is obviously much better that if the voter has to secure his or her own environment. The possibilities of impersonation are much higher by uncontrolled voting, even though modern measures may help reducing the risk by Internet voting.

When the votes are cast by paper ballots and manually counted the process is slow and often inaccurate. Human errors are bound to happen and the verification procedures for disclosing mistakes may vary a lot. Electronic voting, in controlled or uncontrolled environment, has the big advantage of producing correct results fast.

A *transparent* election is secured in polling stations by a fairly simple and compressed process witnessed by observers and the general public. This does not mean that voting in polling stations is always flawless, but correctly implemented there is a paper trail from observed vote till the protocol is signed which can be witnessed and checked even after the elections. Electronic voting has a major disadvantage in that ballots are being stored as electronic information within the computer and the integrity of the vote and the count is only guaranteed by the IT-systems themselves. Measures can be taken to validate the systems and certification schemes may be established, and the requirement for transparency may rest more on the process of acquisition rather than the vote itself. However, all such measures are dependent on a genuine, general trust in the EMB [KV05] and [OB08]. Should the EMB have a will to manipulate the systems to produce a certain result, this can hardly be prevented by independent validation of the system. Validation would be on prototypes and only the EMB can guarantee that the systems used are exact copies of those being validated.

3 Challenges to Voting in Uncontrolled Environment

Uncontrolled voting by mail and by Internet faces severe problems both regarding security and secrecy. On the security issues electronic voting has clear advantages provided modern identification measures are implemented. However, there is no technology available to guarantee that the vote is cast in secrecy free of intimidation and pressure.

3.1 Postal Votes

Postal vote is possibly the most vulnerable method being used today. It has been used to accommodate groups which would otherwise be disenfranchised, but in some countries it has been offered to the electorate in general.

Allowing refugees to vote was an important feature of the election Bosnia and Herzegovina after the war ended in 1995. From 1998 such votes were done by mail. During the elections in 1998 and in 2000 blatant attempts of impersonation of voters were disclosed and even high officials were penalised for assisting in the fraud[3].

Great Britain has in the last elections allowed for postal vote on demand. That means that any voter can request a ballot be sent to his or her address and the voter returns it by mail. During the elections for the Birmingham City Council in 2004 postal voting was used to fraudulently change the results in the wards of Bordesley Green and Aston [BI09]. Persons involved were penalised and some candidates lost the right to stand for elections. A number of techniques were used to manipulate the postal vote, such as requesting the ballot to be sent to addresses where community leaders would fill them in and return them, theft of postal bags, reopening and changing ballots, etc. The election court[4] found that the "evidence of fraud was overwhelming".

3.2 Voting by Internet

Most of the most blatant violations from Bosnia and Herzegovina or from Birmingham could be avoided by a good security system implemented on Internet voting. Electronic voting in uncontrolled environment should, if correctly implemented, protect the integrity of the voting better than postal votes [NO00] and [KV05].

Postal votes may require a signature to an outer envelop and the signature may later be checked if one suspects irregularities. Electronic signatures are being introduced in a number of countries for use in Internet bank transaction, communication with authorities including tax returns etc. So far the most common way of doing this is by pin codes combined with permanent or dynamic passwords. None of these methods offers any guarantee that the person at the screen is the person given the codes, and it is accepted (regardless whether it is legal or not) that person may use an authorisation to actually operate the computer on somebody else's behalf.

Future technology will probably include keys with biometric identification, and at that point in time one may be able to check that the person with the authorisation is present at the computer, but there is no guarantee that the person is alone. In conclusion the practical measures taken against impersonation may be much stronger for Internet voting than by postal votes. The secrecy of the vote can, however, never be guaranteed by any uncontrolled voting.

3.3 International Conventions and Commitments

It is universally accepted that principles of suffrage require a State to establish a system of elections that ensures secrecy of the ballot. Article 25 of the 1966 International Covenant on Civil and Political Rights (ICCPR) provides:

---

[3] The author was Director for Election at the OSCE Mission to Bosnia and Herzegovina in 2000.
[4] In local government elections in Britain, an "election court" is a court consisting of one High Court Judge.

> (b) to vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;

European conventions and commitments are consistent with the ICCPR. Article 3 of Protocol N°1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms similarly provides:

> The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure free expression of the opinion of the people in the choice of the legislature.

The Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, later the OSCE, (29 June 1990) states:

> (5) [The participating States] solemnly declare that among those elements of justice which are essential to the full expression of the inherent dignity and of the equal and inalienable rights of all human beings are the following:
>
> (5.1) free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure, under conditions which ensure in practice the free expression of the opinion of the electors in the choice of their representatives; …..
>
> (7) to ensure that the will of the people serves as the basis of the authority of government, the participating States will
>
> …
>
> (7.4) ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public;

These conventions and documents state the obligation of a State to hold free elections by a secret ballot.

Election observer missions to transfer democracies have normally commented upon breach of secrecy when being observed in polling stations. So-called family voting is common. This is voting where family members enter the secrecy booth together. There may be no sign of intimidation, but it is still reported as a violation of the rules. Observer missions have been less concerned with the possibility of team work when an uncontrolled ballot has been filled in, even though the aspect has been mentioned.

Some countries interprets the commitments to mean that all votes cast should be secret whereas other would hold it for sufficient if a controlled environment is being offered to all voters who want to cast a secret vote.

4 Aspects of a Secret Vote

Postal voting and voting by the Internet do not guarantee a secret vote. Even with strong instructions and guidelines, there will be no guarantee that a ballot has been filled in secret with the marked ballot out of the view of others. In the following various aspects of allowing for a non-secret vote are discussed.

4.1 Tracing Votes Cast in Paper Based Systems

A secret vote would mean that nobody witness any acts where the voter's choice is being made. In addition the system should insure that a vote already cast cannot be traced back to the voter.

In some traditions, e.g. in the UK and in some former British colonies, the ballots are numbered and the voter's name is entered on the ballot stub with a corresponding number. This enables election officials to trace votes of individuals after the elections. Such a tracking would be a serious election violation and the secrecy may be maintained in countries with an election administration with full integrity. The justification for the numbers is that it may be used when investigating petitions relating to election fraud, and only a judge can allow for the secrecy to be broken. As one of the few cases in recent years such a decision was issued in the UK during the investigation of the Birmingham case mentioned earlier.

If very small batches of ballots are accounted for it may be a breach of secrecy. Many countries would therefore have a minimum number of ballots (e.g. fifty) which can be counted in an identifiable batch.

For early voting or ballots cast in a polling station where the voter is not registered so-called tendered ballots are used to prevent multiple voting or to check the voting right of a non-listed voter. The ballot is called tendered because it is not immediately accepted. It will have to be verified against the voter register and against any multiple voting by the voter before being accepted. The ballot is put in an unmarked envelop which in turn is entered into an envelope where the voter's name and ID number and possibly a signature is written on the outside. During the count the outer envelope is checked against the voter registers and if it is accepted as a good vote the outer envelope is broken and the inner envelope is entered into a box. After the verification process the box is emptied, the ballots removed from the neutral envelopes and the votes are counted.

If the procedure is followed, the secrecy of the voters is maintained. This process can be observed by candidate representatives, but it also dependents on a certain level of trust. Checking certain voters' ballots would be technically possible, but clearly a serious election offence.

4.2 Why Secret Votes?

The reason for the secrecy is first of all that the vote should be cast without any interference, intimidation or pressure. The ballot is the voter's own personal expression of his or her will. Without having any way of checking what an individual has voted buying votes will be practically impossible, even though strong community leaders may be able to direct a village or neighbourhood without having the possibility to check each vote individually.[5]

The concept of a secret vote is so well rooted with most people in old democracies. During the upbringing, in schools and in participation in the civic society the secrecy of the vote is taken for granted. A very strong protection of the secrecy may not be felt to be needed any more because any voter who wants the secrecy be protected will be able to cast the vote free from pressure.

In transfer democracies so-called family voting (family members entering the secrecy booth together) used to be common. This did not necessarily mean that voters were intimidated, but the vote was clearly less personal than if cast in solitude. Not least by encouragement from observer missions and the international community in general stricter rules have been implemented in a number of countries. In the elections in the Palestinian territory in January 2005 and in January 2006 the training of election staff had improved tremendously compared to the elections in 1996[6], and family voting was reduced if not eliminated. The long term effect of a strict regime will hopefully be a more profound understanding of the personal responsibility every voter has for the vote.

In Russia and in Romania it was common in early elections after the change to multi party elections (1992 and 1993) to observe large groups of voters filling in the ballots together outside the booth, at least in some districts[7]. The reasons given could be the complexity and lack of light in the booth etc. Intimidation was not necessarily observed or reported, but obviously in such circumstances it would have been possible for a community leader (a mayor, a kolkhoz director etc) with his or her mere presence to control the voting.

In the cases above there may not be a strong wish by the voter to hide his or her vote from either a family member or from all other people present for that matter. On the other hand the environment does not demonstrate the personal nature of the vote and it does not encourage people to insist on a secret ballot.

The conclusion is that the concept of a secret vote is not an obvious one. In order of having the concept generally accepted the secrecy would have to be enforced.

---

[5] Examples of retaliation on a whole village or threats of the same has been observed in some countries though, e.g in Zimbabwe in 2003 and 2005 [KV06] and [KV07].
[6] See election observation reports from the EU and NDI.
[7] See the reports of the Norwegian Helsinki Committee on elections in Romania in September 1992 and in Russia in December 1993.

4.3 Effects of Non-Secret Votes

When discussing the uncontrolled vote as an offer to all voters one has to consider the variety of family structures and community structures that exist in any society. In the Birmingham case the judge wrote: "It should be merely noted that undue influence remains a huge and apparently irradicable problem with postal voting, especially in vulnerable communities, including some of those with ethnic minority electors" [BI09]. This is a comment not on the fraud which the case was concerned with but rather the general problem of a non-secret vote. The Birmingham case included minority communities with traditional family structures. The problem may, however, be valid in a large variety of families.

In a many families the *pater familias* (or any family head) may do all the paperwork and mark all ballots for the whole family, only asking family members to sign the forms or provide the electronic signature where required. Members of the household may accept this as a simple arrangement for paying bills, do tax return, etc and therefore fail to see a problem if the same arrangement is followed for voting. It could happen that a family member would want to cast an individual vote, but due to a traditional respect for the head of the family he or she would hesitate to demand to fill the ballot out in person and in secrecy. In addition to the possibilities of "family voting", there may also be possibilities for a coordinated effort by community leaders which go beyond legitimate assistance and which may include breach of secrecy.

This has a self strengthening effect: Voting will not have any focus in the family because the family head is always taking care of it. As a consequence political consciousness may be reduced and a wish for casting a secret vote may never be expressed, even when a family head would have no objection to it. The problem is not so much the cases where a family member insists on a personal, secret vote, but rather where the voting is seen as any other paperwork and does not get any special attention. The opportunity of building up consciousness about the basics of representative democracies is weakened or lost.

The main source for the understanding of a personal and secret vote has been the strict regulation of the vote in polling stations. Should this educational element be less prominent it may happen that new generations of voters would lose out on the personal aspect of the vote. The effects may be stronger for groups of immigrants from countries where family voting is an almost legitimate tradition even in polling stations, but the risk is there for all groups. Internet voting is often said to be more attractive for young people. If so, young people may then choose to vote together and a group pressure may easily develop.

4.4 Proposals to Reduce the Negatives Effects of Uncontrolled Voting

Some measures may be taken to reduce the negative effects of uncontrolled voting. One is to allow for uncontrolled voting only prior to the elections, not on election day (as in Estonia in 2005). In such case one may build into the system a legal possibility to regret the vote and to override the vote on election day in the polling station. This can be implemented by regarding the postal ballot as tendered ballot which has to be checked against the voter register and the votes cast on election day before being counted.

By early Internet voting the voter may be given a possibility to change his or her vote either on the Internet or by casting a ballot in person on election day. That would offer a possibility to such voters who might have been under pressure by family members, community leaders or friends to cast a particular Internet vote to override the vote on election day in controlled environment. This would only help in such cases where the voter is conscious enough to want to exercise the right to a secret ballot. To accommodate such a possibility technically, a link between the ballot and the voter has to be maintained until the final verification. The verification of whether the ballot is to be counted or if it is overridden by a later vote has to be done first. In the case the Internet vote is to be counted the link between ballot and voter is broken for good, and only then the vote can be counted. Such a system can maintain the secrecy of the vote provided any manipulation by insiders can be ruled out.

Should uncontrolled voting be common it is extremely important that strictly controlled polling stations are available on Election Day for all those who choose to cast a vote in guaranteed secrecy. The danger by a successful introduction of uncontrolled voting is that there is an administrative pressure to reduce the number of polling stations. One may also experience a more relaxed secrecy within the polling stations since the officials would know that the votes are generally not secret any more, even though the need is for more not less control in the polling stations.

A measure which is taken by some countries is to require that the voter, and sometimes even witnesses, sign a statement confirming that the vote is a personal one and that the ballot is cast in secrecy. There may also be penalties to any violations of the secrecy. Such measures may have an effect in particular in cases where the voter wants to protect the vote. To what degree it also effect the less conscious uncontrolled voting may be much more uncertain.

If and when voting in uncontrolled environment becomes an offer to all voters the role of the schools, election administrators and NGOs in educating new generations in the secrecy of the vote will be of paramount importance. Without the direct illustration provided by voting in a polling station the educational challenge will be tremendous.

4.5 Alternatives to Voting in Uncontrolled Environment

The main reason for introducing postal and Internet voting is to strengthen the participation in elections – either by reversing a negative trend or by even increasing the election turnout. In addition in particular Internet voting has attractive features by providing an immediate and reliable count and the long term costs may be reduced.

Some of these effects may be achieved by introducing the same IT based technology but by making it available only in controlled environment. Voters could be offered extensive possibilities for early voting in controlled environment where the secrecy of the vote is guaranteed. In addition there would be staff available to supervise in the use of the Internet, and even paper ballots may be offered.

For young people such an alternative may still be attractive even though the availability arguably would be less than an Internet service accessible from home.An electronic possibility for controlled early voting would have the same advantages regarding the speed and accuracy of count as regular Internet voting. The costs may be higher, though, since the offer is dependent of staff.

Compared to postal votes electronic voting (both controlled and uncontrolled) would have one big advantage in countries where the time from an election is announced to the election day is short, e.g. in the UK. Electronic voting would reduce the turnaround time now being used for requesting a ballot, printing, distributing ballots and returning them, and the time people can actually cast an early vote would be longer. A controlled electronic early vote may therefore have at least the same effect on turnout as the present postal vote system.

Early voting arrangements even in controlled environment have been criticised by international observer missions to for example Belarus. The basis has been the lack of transparency, pressure on voters to cast an early vote (which 31% of those voting did in the 19 March 2006 elections) and the shortcomings in the records kept from the process[8]. However, early non-controlled voting would represent a much higher risk to the integrity of the vote wherever the election management body does not enjoy full confidence from all parties involved.

5 Conclusions

Voting by mail has become common for groups who would otherwise be disenfranchised. A few countries have adopted postal votes as a choice for any voter. Voting by Internet is implemented in few countries and is being planned by more. Serious security issues and concerns of trust and transparency may be solved, at least in countries where the elections management body is above any doubts regarding their integrity. However, the secrecy of an uncontrolled vote cannot be guaranteed. Even if there is a possibility to regret an uncontrolled vote and vote again in a polling station on election day, the free choice may be only theoretical for groups of voters.

---

[8] See the OSCE/ODIHR statement of preliminary findings issued on 20 March 2006 on the Belarus Presidential elections.

Before Internet voting is opened for the whole electorate governments and inter-governmental organisations should have a thorough discussion about the possible effects of the lack of secrecy of the vote. By the development towards more voting from home the concept of election may change without a real discussion of how that may weaken the voters' consciousness of a secret and personal vote. The lack of protection may not only involve common risks of intimidation and trading of votes, but it may lead to less understanding of the personal aspect of the vote for large groups and young voters may in particular lose out on the educational aspect of a secret, controlled vote.

In this discussion early voting in controlled environment readily available to all voters with the most modern technology may be seen as an attractive alternative. Such alternative may offer the same efficiency and accuracy in the results tabulation, it may offer modern user interfaces, but it will require more people and possibly be more expensive to maintain.

Literature

[NO00] Working Group under the Norwegian Ministry for Local Government: Elektronisk stemmegivning – utfordringer og muligheter. Kommunal- og regiondepartemenet. Oslo 2006. www.dep.no/krd/norsk/dok/andre_dok/rapporter/016051-220023/dok-bn.html.

[UK01] Electoral Commission of the UK: Turnout. How many, who and why? London 2005.

[CE02] Council of Europe. Recommendation adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies. Rec (2004) 11.

[CE03] Council of Europe. Report on the compatibility of remote and electronic voting with the standards of the Council of Europe. Adopted by the Venice Commission at its 58th Plenary Session. Venice 2004.

[OD04] OSCE/ODIHR: Elections Observation Handbook 5th edition. Warsaw 2005.

[KV05] Vollan, K: Observing Electronic Voting. Norwegian Institute for Human Rights. University of Oslo. NORDEM Report No 15/2005. www.humanrights.uio.no/ forskning/publ/publikasjonsliste.html#nr

[KV06] Vollan, K: Zimbabwe: Presidential Elections 2002. Norwegian Institute for Human Rights. University of Oslo. NORDEM Report No 05/2002.

[KV07] Vollan, K: Zimbabwe: Parliamentary Elections March 2005. Norwegian Institute for Human Rights. University of Oslo. NORDEM Report No 11/2005.

[OB08] Oostveen, A-M and P. v. D. Besselaar: Security as Brief. User's perceptions on the security of electronic voting systems. ESF TED Conference on Electronic Voting.

[BI09] Election Court in Birmingham: In the matter of a Local Government Election for the Bordesley Green and Aston Wards of Birmingham City Council Held on 10 June 2004. The Court's judgment. Birmingham 2005.

Coercion-Resistant Electronic Elections with Observer

Jörn Schweisgut

Mathematical Institute
University of Giessen
Arndtstraße 2
D-35392 Giessen, Germany
Joern.Schweisgut@math.uni-giessen.de

Abstract: We introduce an electronic election scheme, that is coercion-resistant, a notion introduced by Juels et al. in [JCJ05]. In our scheme we encrypt the credentials that serve as an authorisation to vote during registration. By using a MIX-cascade we can omit one time-consuming plaintext equivalence test in the tallying. In addition, the observer facilitates registration and voting for the benefit of the voter. Pseudonymisation of the ciphertexts during the voting period implies a permanent secrecy of the submitted votes.

1 Introduction

In 2000 Hirt and Sako [HS00] presented the first electronic voting scheme in which voters were not able to prove their voting decision. This so-called receipt-freeness was achieved under the unrealistic assumption of an untappable channel from each authority to each voter. To solve this problem, Magkos et al. [MBC01] introduced an election scheme in 2001 which is based on a tamper-proof device, a so-called observer. That system has been improved in the following in [Sch06].

Besides the long unsolved problem of receipt-freeness, there are further possibilities for an attack on electronic elections, which were described by Juels et al. in [JCJ05] in 2005. They summed up these attacks by the notion of coercion-resistance and proposed a first coercion-resistant voting scheme. In this paper, an election scheme is presented, which is based on the usage of credentials as a proof of authorisation to vote. The tallying is more efficient than in the scheme by Juels et al. and minimises the voter's effort in the registration and voting phase by employment of an observer.

Even if the encryption was broken the receipt-freeness would be lost but the secrecy of the votes could be guaranteed due to the pseudonymisation, nevertheless.

2 An efficient coercion-resistant observer-based election scheme

For the sake of concreteness, we describe in our paper an electronic voting scheme with a non-malleable ElGamal encryption. The scheme also works with other encryption-systems, e.g. Cramer-Shoup (cp. [CS98]) or Modified-ElGamal (cp. [JCJ05]).

2.1 Setup

The MIX-servers define together a multiplicative group G with prime order $|G|=:q$ and a generator g of G. Then they all generate an ElGamal key pair (s,h) with $h=g^s$ (cp. [Ped91]). Each authority A_j receives a share s_j of s in a (t,n)-threshold secret-sharing-scheme and is publicly committed to this share by $h_j = g^{s_j}$. This key h is published as the public-key of the voting-authorities.

2.2 Registration

Each voter V_i, $(i=1,...,n)$, is informed by the authorities, goes to the registration office and authenticates himself towards the registrars. Then the observer is given to the voter.

The voter chooses a random value $z_V \in_R Z_q$ and computes $h_V = g^{z_V}$ as a public share of z_V. This value h_V is stored on the observer. It is important that the observer itself does not know z_V.

The registrars create a probabilistic encryption $E(\sigma)$ of a random string $\sigma \in_R G$ with the public-key h of the authorities in a distributed threshold manner (cp. [GJKR99]). This ciphertext is transferred to the voter and stored on the voter's observer. The registration authorities re-encrypt $E(\sigma)$ and prove to the voter, that the obtained value $E'(E(\sigma))$ is a correct re-encryption of the transferred ciphertext. In order to prevent the voter from transferring this proof we therefore use a designated-verifier proof (cp. [JSI96]). In addition to $E(\sigma)$ the voter creates a fake credential σ' and encrypts it with the public-key of the voting authorities. This value is also stored on the observer as well as the public-key of the authorities.

At the end of the registration-phase a list $\boldsymbol{V}$ of the voter's credentials is published by the registrars via a robust, verifiable decryption-MIX-cascade of the voting authorities.

2.3 Voting

The votes are decrypted by the MIX-cascade in the tallying and published as plaintexts. Therefore, we can choose a representation of the candidates that enables us to simply tally the votes by adding the values. The candidates are described in a number system with the number of candidates n_L as its basis. Let be $\boldsymbol{L} = (m_1,\ldots,m_{n_L}) = (1, n_L, n_L^2,\ldots,n_L^{n_L-1})$ the set of candidates.

Each voter chooses random numbers $a,a' \in_R Z_q$ and encrypts his candidate choice m out of $\boldsymbol{L}$: $(x,y)=(g^a,h^a m)$. Furthermore, he computes $g^{a'}$. These values are sent to the observer which chooses random values $b,b' \in_R Z_q$ and re-encrypts the ciphertext:

$$(x',y')=(g^b g^a, h^b h^a m).$$

In addition to this, the observer re-encrypts the stored ciphertext $E(\sigma)$ of the credential with the public-key of the authorities and obtains $E''(E(\sigma))$. It calculates $g^{a'+b'}$ and the necessary value for the non-malleability

$$b \cdot H(g,x',y',g^{a'+b'},E''(E(\sigma)))+b'.$$

The cryptographic hash-function H serves as a challenge in the non-interactive zero-knowledge proof of non-malleability.

The observer sends

$$(x',y',g^{a'+b'},b \cdot H(g,x',y',g^{a'+b'},E''(E(\sigma)))+b',E''(E(\sigma)))$$

to the voter.

If the observer works correctly the voter can compute (g^b,h^b) from it. Then the voter can complete the non-interactive zero-knowledge-proof of non-malleability and independent vote-creation respectively:

$$(a+b)H(g,x',y',g^{a'+b'},E''(E(\sigma)))+(a'+b').$$

Without any knowledge of the used values a and b it is impossible to create this message (cp. [TY98]).

In order not to stress the measure of confidence in the observer, the observer proves correct encryption in a designated-verifier proof to the voter.

The voter has to prove publicly, that he has encrypted a valid candidate choice. This can be done e.g. by a non-interactive witness-indistinguishable proof P (cp. [CDS94]). If not, he could cast any message as a vote, which would not be tallied, but its value could be used as a receipt towards a coercer. This does not mean that the voter cannot void his vote. It is possible that one option on the candidate list is "cancel vote".

Then the encrypted non-malleable ElGamal message together with the encrypted credential as an authorisation and the proof P is:

$$E(m)=(x',y',g^{a'+b'},(a+b)H(g,x',y',g^{a'+b'},E''(E(\sigma)))+(a'+b'),E''(E(\sigma)),P).$$

The voter sends all this to the electronic bulletin board, a publicly readable memory to which everyone can append but not erase or alter data.

Therefore, the zero-knowledge proof of non-malleability and the proof of a correct candidate choice are publicly verifiable.

The messages from the voters to the bulletin board have to be sent via an anonymous channel. Such a channel can be achieved by employment of a MIX-cascade. To guarantee a permanent secrecy of the votes, the messages from the voters have to be secured by enabling voters to cast ballots in public places or from any point of the net. Thereby, the votes are mixed with other ones even if the encryption and thus the anonymity of the MIX-cascade is broken.

2.4 Tallying

Votes without a valid zero-knowledge proof of non-malleability or without a valid proof *P* are ignored. According to a predetermined policy, the votes are ignored that have been cast together with equal credentials, i.e. equivalent credential ciphertexts. That means that at most one vote per credential will be tallied. To decide whether two ciphertexts are encryptions of the same underlying credential, a pairwise plaintext equivalence test (cp. [JJ00]) is used. Afterwards the votes pass the verifiable robust decryption-MIX-cascade. Thereby, the parts of the message that include the credential and the vote are not separately but synchronously permutated. The output of the MIX-cascade is a randomly permutated list of pairs, each pair consisting of a plaintext-vote and a credential. The credentials are compared with the list *V* of authorised credentials. Votes without valid credentials are deleted. The remaining votes are publicly tallied.

3 Criteria and Analysis

Up to now there have been no common criteria for democratic electronic elections. But it would be wise if the electronic elections fulfil at least the requirements that are set on conventional secret ballot elections. In addition there are some further requirements that derive from the media (e.g. correctness, verifiability, non-malleability and coercion-resistance).

The described voting scheme fulfils all the demands that are put up for traditional secret ballot election and to a great extend the requirements that have been set up for electronic voting schemes so far.

3.1 Authorization, Unforgeability, Single vote

The verification of the authorization and the unforgeability of votes are guaranteed by comparing the credentials with the list of valid credentials. After the registration the valid credentials are anonymised and published via a verifiable MIX-cascade. With this list, everybody can check if a message comes from an authorized voter, but it is impossible to find out from which one. Unauthorized messages are ignored.

The unforgeability of votes is based on the security of the scheme used to encrypt the credentials. Such public-key encryptions are not indefinitely secure. On the other hand one does not need a perfect secure encryption (i.e. a one-time-pad) as a break of the scheme is only advantageous for an adversary in the period before the actual tallying.

If only the first cast votes with correct credentials are considered for the tallying and later submitted votes of the same voter are declared invalid and are erased, then it is guaranteed that one voter can only cast one valid vote.

3.2 Verifiability

As the bulletin board is publicly readable, everybody can prove the non-malleability (independent vote-creation) and that the votes contain valid elements of the candidate list. The plaintext-equivalence-tests for the encrypted credentials to prevent double-voting are also publicly verifiable. During the tallying the votes are sent through a MIX-cascade and decrypted. So the actual tallying can be done by everyone. This means that the verifiability of the voting schemes derives directly from the verifiability of the MIX-cascade.

3.3 Correctness

The correctness of the tallying is guaranteed if all voters are able to cast the vote of their choice, i.e. all voters can understand and check the encryption of the observer. This is ensured by the designated-verifier- and the witness-indistinguishable-proof, the verifiability of the MIX-cascade and the public tallying of the plaintext votes.

3.4 Honesty, Robustness

A dishonest voter is not able to submit an invalid vote that is accepted and tallied. On the one hand he has to include a proof, that the cast vote contains a valid candidate choice. On the other hand the votes are decrypted and invalid votes will be ignored.

It is due to the verification of each action of each MIX-Server that fraudulent authorities can be identified and excluded. As long as there are not more than a certain threshold of dishonest MIX-servers the election can be completed without them. Therefore the voting scheme is robust.

3.5 Expenses

The complexity of communication depends on the used proofs, i.e. the designated-verifier proof, the zero-knowledge-proof of non-malleability and the witness-indistinguishable-proof of the valid choice. These proofs can be efficiently implemented and the communication costs are independent of the number of authorities as well as of the number of candidate choices.

The registration can be done for several elections. The efforts on the side of the voters are acceptable.

3.6 Anonymity

The anonymity of each voter is guaranteed if the used credential cannot be traced back to the voter. That is the case in this voting scheme, as the votes are cast via an anonymous channel (MIX-cascade) *and* the voters can cast their votes from any point of the net. It is impossible to find out which choice a voter has made, even whether a specific voter has cast a vote.

Only those who know the credential of a voter prior to the tallying may find out *if* a voter has submitted his message. Assuming that the used encryption would be broken anytime after the tallying, then the credentials and the anonymous channel still conceal the relation between the votes and the voters - as long as the voter has not given his correct credential away prior to the tallying.

3.7 Independent vote-creation

It is impossible to copy a vote of another voter, because he has to prove in zero-knowledge that he knows the randomness used to encrypt the vote. Due to the non-malleability (i.e. chosen-ciphertext-security) of the encryption, it is impossible for an adversary to cast a vote that bears a known relation to a vote of another voter.

3.8 Coercion-resistance

The voting scheme is receipt-free, i.e. it is impossible that a voter creates a receipt which indicates his choice. If he was able to create one, he would be coercible or corruptible. It is even thinkable that the voter is controlled by an adversary and casts the vote the adversary wants him to. As long as he uses a fake credential, this vote will not be tallied and the voter can still cast his vote he wants to. In addition to that, the scheme is secure against a randomization attack as it is possible in [HS00], because only *one* candidate choice has to be encrypted to construct and cast a vote. It is not even noticeable if a voter has cast a vote and that is why it is impossible to force a voter to abstain from the election. Therefore the scheme is coercion-resistant.

4 Conclusion

The electronic voting scheme fulfils the requirements set on democratic electronic elections in section 3 including coercion-resistance.

If the encryption-key of the authorities was compromised, the pseudonymisation would guarantee the secrecy of the votes, unless the voter publishes his pseudonym before the actual tallying takes place.

The observer does not fulfil the "classical" tasks of an observer (cp. [CP92] and [CP93]) but it rather serves as a convenient and secure transport.

If an adversary forces a voter to hand over his observer, then the voter can give him a wrong PIN. That results in the fact that the observer uses the fake-credential. The voter is able to vote without observer even if the adversary has tried to vote with his observer before.

By using the encryption of credentials and the MIX-cascade for the generation of the list of authorised credentials, we can omit one of the time-consuming plaintext-equivalence tests during the tallying.

Only the plaintext-credentials have to be compared.

References

[CDS94] Ronald Cramer, Ivan Damgård and Berry Schoenmakers: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Yvo Desmedt, editor, *CRYPTO '94*, LNCS 839, pages 174-187. Springer, 1994.

[CP92] David Chaum and Torben P. Pedersen: Wallet Databases with Observers: In *CRYPTO '92*, LNCS 740, pages 89-105. Springer, 1992.

[CP93] Ronald Cramer and Torben P. Pedersen: Improved Privacy in Wallets with Observers (Extended Abstract): In *EUROCRYPT '93*, LNCS 765, pages 329-343. Springer, 1993.

[CS98] Ronald Cramer and Victor Shoup: A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack: In Hugo Krawczyk, editor, *CRYPTO '98*, volume 1462 of *LNCS 1462*, pages 13-25. Springer, 1998.

[GJKR99] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin: Secure Distributed Key Generation for Discrete-Log Based Cryptosystems: In *EUROCRYPT '99*, pages 295-310, 1999.

[HS00] Martin Hirt and Kazue Sako: Efficient Receipt-Free Voting Based on Homomorphic Encryption: In *EUROCRYPT '00*, LNCS 1807, pages 539-556. Springer, 2000.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson: Coercion-Resistant Electronic Elections: In *WPES '05*. ACM CCS, November 2005.

[JJ00] Markus Jakobsson and Ari Juels: Mix and Match: Secure Function Evaluation via Ciphertexts: In Tatsuaki Okamoto, editor, *ASIACRYPT '00*, LNCS 1976, pages 162-177. Springer, 2000.

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo: Designated Verifier Proofs and Their Applications: In *EUROCRYPT '96*, LNCS 1070, pages 143-154. Springer, 1996.

[MBC01] Emmanouil Magkos, Mike Burmester, and Vassilios Chrissikopoulos: Receipt-Freeness in Large-Scale Elections without Untappable Channels: In *I3E '01*, IFIP Conference Proceedings 202, pages 683-694. Kluwer, 2001.

[Ped91] Torben P. Pedersen: Non-interactive and information-theoretic secure veriable secret sharing: In *CRYPTO '91*, pages 129-140, 1991.

[Sch06] Jörn Schweisgut: Effiziente elektronische Wahlen mit Observer: In *GI - Sicherheit 2006*, LNI Proceedings P-77. Gesellschaft für Informatik e.V. (GI), February 2006.

[TY98] Yiannis Tsiounis and Moti Yung: On the Security of ElGamal Based Encryption: In *PKC '98*, LNCS 1431, pages 117-134. Springer, 1998.

Session 7: Implementing E-Voting

Maintaining Democratic Values in e-Voting with eVACS®

Carol Boughton

Software Improvements
Unit 20, 16 National Circuit
2600, Barton ACT, Australia
carol@softimp.com.au

Abstract: The principles of equality, secrecy, security and transparency apply to any democratic election system irrespective of whether paper ballots, mechanical or electronic means are used to conduct the election. All these principles were mandated as requirements, designed into, and successfully operated as features of, eVACS®, the electronic voting and counting system used since 2001 by the Australian Capital Territory Electoral Commission. How eVACS® achieves these requirements is described in this paper, with particular emphasis being given to security and transparency and the approaches adopted to ensure verifiability via electronic audit trails.

1 Introduction

All democratic election systems have many features in common no matter where a particular system is applied.

In the UK [Wa02], six principles were initially identified as forming the minimum requirements of a democratic election procedure. Public consultations established wide community support as well as leading to their simplification to three principles.

1. the **doorkeeper** principle: - Each person desirous of voting must be personally and positively identified as an eligible voter and permitted to complete no more than the correct number of ballot papers.

2. the **secrecy** principle**: -** Admitted voters must be permitted to vote in secret.

3. the **verification, tally and audit** principle: - There must be some mechanism to ensure that valid votes, and only valid votes, are received and counted. The system must be sufficiently open and transparent to allow scrutiny of the votes and subsequently the working of the political process.

More recently three democratic values were identified as being essential to any voting system adopted in the USA [To04]:

i) **equality** (of political participation), including racial equality; multi-lingual access; disability access; inter-jurisdictional access (or no differential treatment to voters based on the county or jurisdiction where they reside);

ii) **security** (the resistance of votes and vote totals to fraud and other forms of manipulation); and

iii) **transparency** (the capacity to produce auditable results in which both candidates and voters can justifiably have confidence).

These values or principles of **equality**, **secrecy**, **security** and **transparency**, apply to any democratic election system – no matter whether the election is conducted using paper ballots, mechanical or electronic means. Exactly these requirements were recognised and specified in 2000 for the electronic voting and counting system eVACS®, successfully used by the Australian Capital Territory (ACT) Electoral Commission in the 2001 and subsequent ACT Legislative Assembly elections [El02] [El05]. Descriptions follow on how eVACS® ensures **equality, secrecy, security** and **transparency** with particular emphasis on the approaches adopted to ensure verifiability via eletronic audit trails.

2 Equality

The voting set-up is identical for all users. For the vision impaired, or voters with poor reading skills, audio is provided and, if required, a larger screen. Privacy is maintained by the use of a headset, with voters able to use their own headset or a disposable one. The use of a (special) keypad to record choices/preferences enables voters with a range of physical impairments to vote without assistance. For preferential or proportional election systems in which voters are required to indicate a sequence of numbered preferences, selection of a candidate automatically assigns the next number in the sequence ensuring there are no missing or repeated numbers. Thereby ensuring voters do not unintentionally vote informally.

Other features addressing equality include instructions being provided in the voter's language of choice, as well as the local language of the region, using any alphabet or character set. If permissible by law, voters are able to vote away from their normal polling place. The hardware can be placed to give voters their choice to either sit or stand to vote.

3 Secrecy

Vote secrecy is maintained in five ways. First, the voting screen is positioned so that no other person is able to see a constructed vote. Second, the system fits in a normal (cardboard) voting booth. Third, for the standard arrangement no noise signals are emitted to alert anyone else as to how a voter may be voting.

Fourth, because voters 'navigate the electronic ballot' using the keypad, it is extremely difficult for anyone else to be able to discern who is being voted for. And fifth. a voter can 'hide their vote' if they need to seek assistance from an official.

In addition, all of the equality features (described in Chapter 2) increase the number of people who can vote without assistance, and thereby vote in secret.

4 Security

Security involves a number of design and operational aspects covering software and hardware, including a log of all activities. Automated set-up arrangements ensure that an election is run from a series of auditable write once CDs, and on loading the software, the hard disk/s are reformatted thereby removing any existing operating system and other software. Limited functionality, for voters and officials, means software cannot be modified during an election.

At the polling place each voter is randomly assigned a barcode, from a restricted set of barcodes internally generated by the system. The barcode determines in which election/s a voter is eligible to vote, ensures only completed votes are stored, and identifies incomplete votes if the network is disrupted. Whether a barcode has been used is checked automatically before voting commences and may also be checked manually.

All votes are cast in a public polling place over an isolated LAN with votes only stored on physically secure voting servers. No votes are stored on voting machines used by voters. The votes are stored simultaneouslyin two separate databases to guard against loss of votes due to hardware failure. Additionally, the outcome of a rerun in sequential order of voter keystrokes must match with the voter's choices before a vote is recorded and stored. Downloading of votes at the end of polling requires password and encryption keys, not transmitted to polling place officials until after polling closes. Votes are encrypted and downloaded to two write once CDs with checksum. Both disks have to be loaded into the counting server and match the checksum.

The combined auditing and internal security features ensure a court is able to verify the CDs that were used for a specific election, and that the election result is accurate and has not been tampered with in any way.

4.1 Security of hardware

The election software runs on any hardware that supports the Linux operating system. The degree of in-built security of hardware can vary significantly between equipment. Consequently, there is an emphasis on maximising security via the software with physical security an added feature where available.

Used in the 2004 ACT Legislative Assembly Election, the ROC - Rugged Operations Computer - specially designed for electronic voting [Ro04] [El05], provides advantages over standard PCs in respect of ease of set-up and use, as well as better protection against external damage from liquids, solids, heat and physical damage. Each polling place LAN network is also physically protected against attempts to break into the system.

5 Transparency

In paper based voting systems transparency is managed by having observers/scrutineers present at different stages of the voting and counting processes, such as: empty ballot box and then securing (eg by sealing or locking) the box at the start of polling; ballot boxes remaining secured until after close of poll; only those people who actually attend the polling place are marked off the electoral roll at that polling place; assistance to voters incapable of marking their ballot paper by themselves; only voters place the appropriate ballot papers in the ballot box during polling; emptying of ballot box at the close of polling; counting of ballot papers after close of poll; secure transportation and/or storage of the votes; and recounting of votes.

Electronic voting and counting must, by necessity, change the nature of scrutineering, but computerising the voting and counting processes ought not prevent elections from being transparent, nor prevent scrutineers from observing all aspects of the voting and counting processes. "*A computerised voting and/or counting system is in essence a series of mechanical steps, facilitated by computer hardware and computer programs. A thorough understanding of the way in which the hardware and programs work – the electronic trail – should serve to demonstrate that the system is transparent, and in particular, that 'what goes in is what comes out'*." [Gr03]

There are some activities of scrutineering that are outside the scope of electronic voting. To ensure the anonymity of votes there can be no connection between the voter's details and their vote. Any system for marking people off the electoral roll (either paper or electronic) must be independent of the voting and counting processes. Hence, the observation process to ensure only eligible people vote continues independently of eVACS®.

As with paper ballots, transparency in an electronic election has a number of stages, grouped into five levels, none of which is sufficient by itself to demonstrate the required transparency for an election. Each level of transparency must be completely fulfilled.

In the first level of transparency code is available so others can assure themselves that the software does what it is meant to do and nothing else. The Electoral Commission arranged for independent auditing of the software code used for acceptance testing and then in an election. The audited code was released publicly.

After the 2001 election, researchers from the Australian National University independently verified the counting algorithm and replicated the results of the 2001 ACT Assembly election.

The second level of transparency requires the correct operation of the vote recording and paper ballot data entry processes, and votes counted accurately according to the specified election system. Extensive testing prior to the software being put into service was undertaken, plus acceptance testing by the customer prior to auditing with representatives from political parties and disability groups observing.

For the third level of transparency, the software used for an election can be shown to be exactly the same software that passed first and second levels.

The fourth level of transparency involves Officials demonstrating the in-built features of the closed system ensure the limited functionality cannot be tampered with during use in an election, there is an empty electronic ballot box at start of election, the number of votes (formal/informal) in electronic ballot box, the initial results (for specific polling places), and secure downloading of votes. Downloading of votes is security controlled both to download and when uploading into counting server with encryption of votes, password access and checksums on CDs.

To achieve the fifth level of transparency voters and officials have to be confident that none of the recorded votes are lost, and that only completed votes are recorded. Activities to meet other levels demonstrate the former, while the barcode provided to each voter is used to start and end a voting session and ensure only completed votes are recorded.

In addition, there must be a well-documented 'electronic trail' with all the development artefacts and code available for independent auditing, and the source code published for examination by interested persons.

On the introduction of computer technology as applied to electoral matters in Australia, the then Commonwealth electoral authority's explanation for its reluctance to move too rapidly into computers in 1982 was: *It is absolutely essential not only that an election system be fair, but that it is seen to be fair. The safeguards built into the current system are the product of many years of experience. The full-scale introduction of a new, and much more complicated system could create opportunities for illicit interference, or allegations of such interference, with the electoral process. A completely new security process would have to be developed – one which would be acceptable to the electorate, the candidates and the political parties. (op cit Hansard V.129 1982 1614).* [Mc01]

While new steps in computerisation of the election process have subsequently been taken each year, they have not been submitted, step by step, to parties and candidates for open debate, let alone to the electorate *(page 166 of [Mc01]).*

In Ireland the Commission on Electronic Voting in its first report [Ir04] was unable to recommend use of the chosen electronic voting system because the accuracy and security could not be established as: i) there was not sufficient time to fully test the system, ii) the full source code had not been made available, iii) the version to be used was unknown and therefore the accuracy of the system could not be certified, and there were concerns that secrecy of the vote might be compromised.

In marked contrast, the development and introduction of electronic voting and counting in the Australian Capital Territory occurred with public participation. eVACS® was developed after direct public consultation had led to legislative changes to enable electronic voting and counting, undertaken in association with a Reference Group (with representatives of candidates, political parties and the public) whose members were able to participate in the acceptance testing, and the source code released for public scrutiny before use in an election.

Apart from ensuring a completely transparent electronic trail, elimination of opportunities to tamper with election results is another benefit of electronic voting. Opportunities such as ballot box stuffing, completed ballot papers from a polling place being "lost" and completed ballot papers deliberately inserted in the wrong stack for counting.

Electronic votes cannot be prepared in advance; voting must occur at the polling place and under the direct observation of others. The period when electronic voting is available at any polling place is logged by recording the time whenever the system is activated (start voting) or deactivated (stop voting). A unique barcode must be obtained for each electronic vote.

Electronic votes are stored in duplicate on the voting server at a polling place. The votes are downloaded twice onto separate write once CD-ROMs with a checksum. Details from both CDs are loaded into the counting server and confirmed with the checksum before the votes are added to the counting database. The only option for downloading votes is to download all votes stored on the voting server. Votes for a particular polling place can only be added once to the counting database. A report is available of polling places from which votes have not been imported into the counting database.

Once confirmed by a voter, the limitation of functionality means there is no way to interfere with the content of an electronic vote. There is no means to change the counting program once a specific election has been set-up.

5.1 Recounts and petitions

Recounts were introduced to address the known failings with manual counting of votes, and usually occur when the result of an election is very close. Either the electoral agency or a candidate may seek to have the votes recounted. Also, in some jurisdictions there is a mandatory requirement to recount a proportion of all votes to check the accuracy of the manual count. Whereas in other jurisdictions, a candidate, a voter or the electoral agency may dispute the validity of an election via a petition to a court.

Electronic voting and counting has significant impact on the conduct of recounts and for contesting election outcomes in the courts. The demonstrable accuracy of electronic voting and counting avoids the unnecessary recounts when election results are close. Mandated recounts are not practical with electronic voting, although a random set of votes could be printed and counted manually with less accuracy. With petitions, the issues are not ones of 'who did or did not do what' or 'what was permissible under the election legislation' but whether the computer program used met the appropriate standard of accuracy, reliability and trust. The transparency has to enable a court to independently establish the accuracy, reliability and trust in the election system.

5.2 Electronic voting and voter verifiable audit trails

There is no question about the need for voter verifiable audit trails with electronic voting. However, as per [To04], a 'voter verifiable audit trail' is not synonymous with '*paper* ballot replicas'.

Voter verifiable *paper* audit trails are often cited as the solution to addressing problems encountered with electronic voting in the USA. Yet as has been shown [To04] [El05], whether a voter verifiable paper audit trail is both a practical solution and an effective means of preventing fraud is highly questionable. For example, the tape for a voter verifiable paper audit trail system used in Clark County, Nevada, USA, contain 64 voter verifiable paper ballots from one voting machine, is a strip of 10cm (four inch) wide paper, just under 120 metres in length (318 feet) and "it took a four person team - one counting votes, one verifying and checking for errors and two recording results – about four hours to check one tape, or nearly four minutes per ballot" (photograph in [eo05]). The ability of election officials to accurately determine election results under such circumstances becomes a costly exercise in checking and cross checking.

The USA is not the only country where concerns have been raised about the electronic voting system used. Others are Brazil [Re03] and the NEDAP Powervote system trialled in Ireland [Ir04].

There are some who believe no electronic voting system can be trusted and therefore a paper audit trail is absolutely essential [Me01]. Yet others caution against sacrificing the voting rights of disabled voters and non-English speaking citizens in order to achieve the admirable goal of enhancing election security and transparency [To04]. A voter verifiable paper audit trail is obviously not an option for the vision impaired, poor readers, or voters who cannot read the language of the print out.

Not all the issues raised with electronic voting have been about ensuring votes are recorded accurately at the polling place. There have been reports of vote databases being accessed by the public, uncertified software being used, bug fixing occurring during an election, and equipment being certified without meeting certification requirements [Bl05]. With an appropriate 'voter verifiable audit trail' none of these issues should eventuate.

All of the concerns with electronic voting have arisen where there has been no transparency of the software used nor any serious attention to security issues prior to implementation of the system. In contrast, with eVACS® all of these issues were addressed before the system could be used in an election.

6 Voting is not everything

Maintaining democratic values does not simply apply just to the voting process. The third principle (see Chapter 1 and [Wa02] and [To04]) is to ensure that only valid votes are counted and that the counting process is auditable and transparent. Incorporation of this requirement starts with the set-up for a particular election, and applies equally to all other phases of the election process.

One of the major benefits of electronic elections is the speed at which election results can be determined. To achieve these benefits though, all votes need to be available electronically. Wherever postal voting or the equivalent is available not all votes will be recorded electronically, so there is need for a module that will convert paper votes into electronic votes. Ensuring the same level of accuracy and trust, as for electronic voting, in this conversion process is absolutely critical to ensuring only valid votes are counted.

Having a fully auditable process throughout all phases of an election therefore means that features of transparency and security have been applied to all modules of the eVACS® system, as well as to the interconnections.

6.1 Set-up election

Reference is made in Section 4 to an election being run from a set of auditable write once CDs, and to limited functionality such that the software cannot be modified during an election. In practical terms, the auditable set-up election CD is loaded on to a standalone PC – the set-up election server, and the hard disk reformatted. The set-up election server is then used to generate the voting server and data entry/counting server CDs for a specific election. All CDs are treated with the same degree of protection as ballot papers when being transported but in addition have in-built checksum and encryption features to ensure what was downloaded from one part of the system is identical with what is loaded into another part of the system.

eVACS® is referred to as a ‘closed system’ since there is no interaction with any other software.

6.2 Entry of non-electronic votes

The original eVACS® uses a data entry process for incorporation of non-electronic votes with double entry of the paper ballot details and separate authorisation for editing when entries do not match. Scrutineers are able to observe the entire process.

Developments in scanner technology since 2001 mean there may be an alternative to data entry for managing non-electronic votes, but with two issues that need to be addressed. First, scanning of all paper ballots is not always achievable, and second, particularly when preference numbers are written, not every paper ballot can be scanned with 100% accuracy. As a consequence an auditable and traceable editing process equivalent to that provided for data entry in eVACS® is necessary to ensure that only valid votes are entered and counted.

6.3 Counting and reporting

Counting has different facets that must all be proven to be auditable and transparent: the actual counting algorithm; the process by which electronic votes from different sources are merged for counting; and the actual reporting of results.

Counting algorithms don't just count votes. They determine which votes are valid (or formal) votes. Also, they may need to cater for different interpretations of vote information from votes received by a candidate who dies before the election results are announced. Additionally, when two or more candidates receive the same number of votes there may be a formal separation process that needs to be initiated during the counting process.

For many elections, votes from a number of sources such as different polling places, or electronic and non-electronic votes need to be merged for counting. Ensuring that votes can only be included once is critical to undertaking an accurate count.

Another, often overlooked aspect is the potential for manipulation of results after a count has been undertaken. It is important that the results are not accessible before printing the official election results.

7 A final comment

As with any new development, lessons are learnt from use. In the reviews of each of the 2001 and 2004 elections, enhancements were recommended [El02] [El05] and agreed by the ACT Government [El03]. What is significant about these enhancements is that none sought to change the basic equity, secrecy, security and transparency features designed into the system.

The 2001 recommendation to improve 'the set-up process to automate the loading of election details, particularly candidate names and sound files' was implemented by establishing the set-up election module which turned eVACS® into a 'closed system', thereby further enhancing security.

References

[Bl05] The Official Blackbox Voting Website http://www.blackboxvoting.org/

[eo05] electionline.org "*Recounts: From Punch Cards to Paper Trails"*, 2005 http://www.electionline.org/Portals/1/Publications/ERIPBrief12_FINAL.pdf

[El02] Elections ACT, "*The 2001 ACT Legislative Assembly Electronic Voting and Counting System Review*" ACT Electoral Commission, 2002 at http://www.elections.act.gov.au/Elecvote.html

[El03] Government response to the 2001 ACT Legislative Assembly Electronic Voting and Counting System Review http://www.elections.act.gov.au/EvoteRG.html

[El05] Elections ACT, "*2004 ACT Legislative Assembly Electronic Voting and Counting System Review*" ACT Electoral Commission, 2005 at http://www.elections.act.gov.au/Elecvote.html

[Gr03] Green, Phillip Chapter on "*Transparency and Elections in Australia: The Role of Scrutineers in the Australian Electoral Process"*, in *Realising Democracy: Electoral Law in Australia*, G. Orr, B. Mercurio and G Williams (eds), The Federation Press, 2003, pages 226-228.

[Ir04] Ireland Commission on Electronic Voting First Report on *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System,* 2004 http://www.cev.ie/htm/report/first_report/pdf/00Index.pdf

[Mc01] McGrath, Amy "*The Frauding of Votes*" with an Introduction by Bob Bottom, Tower Books Wholesale, ISBN 0-9587104-3-0, 2004.

[Me01] Mercuri, Rebecca, *Rebecca Mercuri's Statement of Electronic Voting* http://www.notablesoftware.com/RMstatement.html, 2001

[To04] Tokaji, Daniel P: *The Paperless Chase: Electronic Voting and Democratic Values.* Ohio State Public Law Working Paper No. 25, 2004 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=594444

[Re03] Rezende, Pedro AD:*Electronic Voting Systems - Is Brazil ahead of its time?* Paper prepared for the First Workshop on Voter-Verifiable Election Systems Denver, USA, 2003 http://www.cic.unb.br/docentes/pedro/trabs/election.htm

[Ro04] Rugged Operations Computer http://www.roc-solid.com/

[Wa02] Watt, Bob: *Implementing electronic voting in the UK: The legal issues* Office of UK Deputy Prime Minister http://www.odpm.gov.uk/index.asp?id=1133606

Transition to electronic voting and citizen participation

Letizia Caporusso, Carlo Buzzi, Giolo Fele, Pierangelo Peri, Francesca Sartori

Dipartimento di Sociologia e Ricerca Sociale
Università degli Studi di Trento
V. Verdi, 26
38100 Trento, ITALY
provote@soc.unitn.it

Abstract: This paper draws attention to the need of a systematic socio-technical approach to introducing electronic voting and presents early results from a pilot project conducted by the Provincia Autonoma di Trento, Italy. Main features of this experience are the constant monitoring of the social impact and the development of a technological solution in accordance to the suggestions provided by the users themselves. We recommend that no sudden switch to a new form of ballot should be imposed on electors but rather that research is to be fostered in order to uncover and preserve the traditional and symbolic connotations embedded in the act of voting.

1 Introduction

At the time being, the Italian ballot system consists of a paper-and-pencil method and electors are allowed to vote only in the section where they are registered. The vote is expressed by drawing a cross on the symbol of the party and by – eventually – writing down the names of the candidates. During the count contentions do arise, among other reasons, due to the misinterpretation of ballots that are not clearly written or ballots that seem to have been purposely marked in order to be recognized. Citizens who are physically impaired have their vote cast by a person they trust, as no technological support is available to help them vote on their own.

In order to overcome these obstacles as well as to keep the democratic process aligned with the development of e-society, new forms of voting are being considered by the Provincia di Trento which, because of historical and political reasons, benefits from special autonomy status in respect to other Italian areas and can determine by its own legislation how the Council and the President of the province are elected. Such a peculiar condition is favouring a boost in the development of e-government, including a thorough study of the possibility to introduce e-vote for local elections: this project, named ProVotE, was set up since December 2004 and aims at crafting a voting machine that, complying with the standards indicated by the Venice Commission [Ve04], is accepted and easily employable by electors regardless of their age, sex, education and confidence in the use of technology.

2 A systematic approach

ProVotE is characterized by an on-going round-table[1] where representatives of the Provincial Electoral Bureau, researchers from the Centre for Scientific and Technological Research (IRST) and from the Department of Sociology and Social Research of the Università di Trento meet on a regular basis to share developments in each area of expertise and plan systemic activities aimed at testing electors' reactions to a likely, but yet to establish, switch from paper-and-pencil to electronic voting. In the light of the key role played by the study of the social impact, we designed a set of investigations spread over one year in order to get the clearest picture of citizens' beliefs and attitudes toward e-voting before and after the two field tests that took place in May and November 2005.

We define social impact as any change occurring in the symbolic order or in the concrete behaviour of a population in consequence of the exposure to an external stimulus. In investigating the social impact of the introduction of electronic voting we had to consider people's attitudes, expectations, fears and practices *before* they even heard of the possibility of e-voting in their own area, *during* the field tests and some time *after* these trials. The research plan included:

- 8 preliminary focus groups to explore practices and habits related to voting;
- over 2500 telephone interviews to uncover attitudes toward electronic voting and assess the technological ability of the population;
- 160 supervised trials aimed at investigating man-machine interaction by means of both questionnaires and ethnographic observation;
- monitoring of turnout to open trials held in the towns chosen for the first field test;
- a large scale field test in five towns alongside local elections – involving 6950 participants – and a smaller scale follow-up field test with 336 electronic voters;
- analysis of electoral data and comparison of electronic and paper-and-pencil results;
- 1200 telephone interviews four months after the tests to compare attitudes and motivations of those who tried electronic voting and those who did not.

This paper offers a brief account of the main empirical results of the research activities summarised above and underlines the importance of integrating the technological with a sociological perspective, which considers the feedback provided by the end users of electronic voting systems.

[1] The authors acknowledge the support received by the Provincia Autonoma di Trento, especially by the Director of the Electoral Bureau, Patrizia Gentile. We wish to thank Adolfo Villafiorita (IRST) who coordinated the technological team and Giorgia Fasanelli (CRC Trentino).
As with any large project the results presented in this paper are based on the joint work of several people: Andrea Cossu, Lodovica Simionato, Elisa Fanelli analysed qualitative data; Enzo Loner, Cristina Margheri, Michela Frontini analysed surveys.

3 Transition to electronic voting and citizen participation

3.1 The sense of voting and the practices related to elections

The socio-anthropological literature describes the activities associated with elections as *rituals* which enhance the sense of belonging to a civic community [Ed64; Ke88]. Little has been said, however, about the intrinsic value and significance of the act of voting from a subjective standpoint: the *sense* of "having one's say", as well as the *body of practices* related to the expression of the citizens' will, appears to have been widely neglected. A preliminary "qualitative" study was therefore aimed at unveiling the entangled mixture of symbolic and material elements that come into play in the apparently ordinary act of casting a vote.

The focus groups portrayed a rather customary and standardized schedule of the day of elections: people show preferences about the time of day devoted to voting (i.e: early in the morning or late at night to fit with Sunday outings, rather than just before or just after Holy Mass); which might result in queues and a potential intolerance towards any innovation, should it imply a longer time to mark the ballots. The habit of going to vote together with relatives also appears to be rather widespread, in the main if going to the polling station requires a means of transport: the presence of younger people in family groups going together to cast their ballots might then be crucial to reinforce institutional tuition and to bridge the technological gap between generations, should electronic voting be extensively introduced.

More considerations pertain electors' awareness of their ability to vote "properly": whereas paper ballot is considered an easy, automatic act in which the chance of making mistakes is minimal, the idea of voting electronically evokes more perplexities. The perceived social impact can be summarised in the following key issues, which need to be taken into careful consideration, as beliefs often anticipate or even modify the course of future events:

a. interviewees believe that e-voting will have no effect in increasing the turn-out
b. interviewees fear that costs for elections will increase, compared to paper ballots
c. interviewees project their worries onto a specific segment of population (senior citizens) and fear that this social group might be, though indirectly, deprived of the right to vote
d. interviewees reckon age will impact more than educational capital or technological ability
e. a general distrust in politics and a feeling of uselessness of one's vote are often expressed, which, according to the interviewees, might result in an apathetic or critical attitude toward innovations in such a delicate matter.

Nonetheless, the informants (especially the youngest) also brought evidence of some hindrance experienced in the choice of candidates with the paper-and-pencil method: this requires to write down the names properly and correctly to avoid having the vote invalidated, which gives rise to frequent undervoting.

Some practices related to paper voting emerged, such as the frequent use of facsimiles, which are mailed by candidates and show how to fill in the ballot. In the light of such a habit, keeping the visual layout of the touchscreen consistent to that reproduced on paper does not require a major change in the electors' expectations and is welcomed by all interviewees.

A surprising result of this preliminary investigation relates to the citizens' opinion about the use of a printer that allows electors to verify their ballot [e.g. Me02]: unexpectedly, they seem to consider it an unnecessary token which does not fit with the idea they have of "electronic" voting. They argue that the cost of printing and counting ballot proofs will equal or exceed the expense of traditional ballots without suggesting the same feeling of control and trust that the paper offers.

At the same time it is important to stress that the confidence of electors in the traditional procedure is also influenced by the fact that anyone has the chance to be a scrutinizer or a list representative and therefore to be protagonist and witness of the entire process: the switch from material to "immaterial" practices seems to deprive the community of the direct contact with the ballots.

By interviewing the scrutinizers, further evidence related to the need of trust also emerged:

a. trusting that one's ballot is personal and secret (thus guaranteeing one's freedom of choice)
b. trusting that each and every vote is actually counted (i.e., not "thrown away")
c. trusting that the ballot count truly respects the voter's will (also by being available for further controls and re-counts)

The board of scrutinizers appears to be a peculiar kind of organization, in the sense that it is formed and disbanded on the same day of elections: it learns to optimize time and procedures while already in action and often shows more flexibility and discretionary power than it'd be strictly allowed by norms and legislation, in order to prevent mistakes due to fatigue or lack of attention. Its "professional culture" is easy to acquire and available to almost anyone: the practices related to casting a ballot become, in the course of election day, a well-oiled "machine". When this voting machine works, be it paper-based or electronic, it should become sort of invisible: its efficiency and its acceptance by the citizenry is signified by its *disappearance* in the sense that it becomes a *routine* taken for granted, and not an "issue".

At present, the complex and time-consuming bureaucratic procedures related to data management are described as cumbersome and old-fashioned: a simplification of the procedures related to electors identification, ballots count and register filling would definitely be welcome.

Above all, both scrutinizers and citizens explicitly and implicitly stress the need for adequate information: switching to electronic voting implies a significant change in a long established and framed routine. A new habit has to be created from scratch and it cannot be learned "by trial and error" as one might find acceptable in other technological settings. To smooth the transition to e-voting this preliminary study suggested that:

- the touchscreen should show some continuity with the paper ballot to reduce the need for cognitive re-adaptation;
- appropriate instruction should be ensured to both electors and scrutinizers: their confidence with the new system can be enhanced by open trials;
- special consideration should be granted to senior citizens: the care that institutions show towards this group will be reflected in the appraisals of many others.

3.2 Are we ready to vote electronically? Attitudes and technical skills

Alongside the "qualitative" investigation, a preliminary "quantitative" survey was carried out by means of telephone interviewing to assess the interest of the population in changing the voting procedures. The sample (2561 respondents) was representative of the adult population of Trentino, controlling for age, sex and geographical distribution. The aim of this study was to consider attitudes towards electronic voting as well as practical technological ability. The latter was measured by an index created on the basis of statements related to the use of common electronic appliances requiring skills similar to those needed for e-voting. Approximately 10% of the respondents turned out to be barely familiar with technology and a further 6% to be very unacquainted with menu-like procedures. Those who might be impaired in the use of electronic means are mostly elderly people, retired, with no or very little education. The attitudes toward electronic voting, or rather, to whatever the respondents thought electronic voting to be (as they had never experienced it in elections), are summarised in Figure 1.

How much do you agree with the following sentences?	**%**
• Voting procedures should inevitably be changed, sooner or later	70,3
• Electronic voting is a good idea, but I believe it'd be difficult to implement	58,2
• Electronic voting might eliminate contentions in interpreting voters' will	55,9
• Electronic voting might increase abstentions	54,4
• Electronic voting might lower the mistakes that today cause ballots to be invalidated	53,2
• Electronic voting is a dangerous solution as it'd be prone to vote tallying that can't be easily demonstrated	42,0
• With electronic voting there'd be no tangible proof of my vote	36,5
• Electronic voting wouldn't fully guarantee that the ballot is secret	36,1
• People are ready to switch to electronic voting	28,2
• I don't trust technology and therefore I don't trust electronic voting	27,9

Figure 1: Attitudes toward electronic voting (% of answers "agree" and "strongly agree", *n*=2561)

These attitudes confirm some of the beliefs already found via the focus groups, such as the fear that some segments of the population might not be ready to vote electronically, thus increasing abstentions; the desire that certain common mistakes and controversies will be eliminated and a feeling of the inevitability of change. However, citizens are on the whole in favour of voting electronically even in the near future, as Figure 2 shows. It's mainly professionals, students, educated people approximately below 50 years of age who are enthusiastic about e-voting (more than 65% are in favour), whereas elderly, retired citizens with no education show very little interest (less than 40% are in favour).

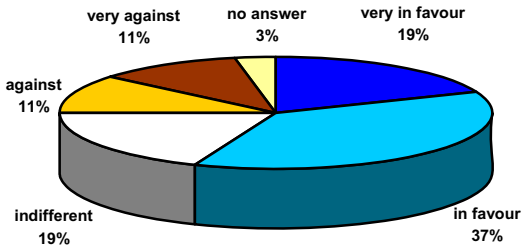


Figure 2: “Should electronic voting be adopted for the next provincial elections, would you be in favour or against this idea?” (%, *n*=2561)

The voters’ openness toward voting electronically in the next elections appears to be more related to their attitudes than to specific socio-demographic characteristics: sex, social class, education and even age have little or no impact on the will to use an electronic ballot, when technological ability and attitudes are controlled for. Young people are more inclined to technology but seem to be little interested in politics; on the other hand, senior citizens are less confident with electronic methods but are very motivated towards participating in elections, as they feel it to be a duty, not just a right. Education level has a limited direct impact on the will to vote electronically: only those who received no education, controlling for age and technological ability, are significantly less in favour. The size and the level of development of a town also have, perhaps unexpectedly, almost no influence: this indicates that smaller, rural and peripheral locations are likely to accept a switch to electronic voting at the same pace as urban areas, despite being conditioned by more “traditionalism”. What really determines the acceptance of electronic voting is the image of the strengths and pitfalls of the system: trusting or distrusting this unknown and never experienced means being the most powerful incitement or deterrent.

The quantitative preliminary study also suggested that:

- citizens are generally in favour of adopting electronic voting and their expectations are mostly positive, though some doubts remain and should be cleared before this new method is adopted;
- the fear of not being ready for the change is challenged by the widespread use of electronic appliances that require skills similar to those necessary to vote electronically;
- for a campaign to introduce e-voting to be successful, it should stress the benefits and assure electors that safety is guaranteed;
- voting machines should be adapted to the electors’ needs (rather than expecting electors to adapt to voting machines) and citizens should be aware of this effort.

Once a prototype of the voting machine was ready, trials and simulations were organized in the five towns chosen for the first large-scale field test scheduled to be performed during local elections. To try the electronic ballot with the most disadvantaged social group, a sample of 80 senior citizens was randomly chosen from the registries, ensuring that their educational level was very low or null; a reference group of further 80 young and middle-aged people was also invited to the tests, on condition that they possessed at most a high school diploma. Participants in the simulation filled in a questionnaire before and after the trials and were video-recorded during the test. As a result:

- the visual layout of the screen, i.e. the position of "buttons" and the size of characters was modified
- the choice of preferences and, generally speaking, man-machine interaction, were optimized by observing how people "naturally" tend to cast a vote by means of a touchscreen.

The flyer with instructions for the correct use of the new form of ballot were also submitted to non-experts for concept-testing via focus-groups and in-depth interviewing.

This complex but continuous exchange between the efforts of the technological team, the law standards required and guaranteed by the electoral bureau and the contribution of citizens themselves helped to develop a low-impact system which was ready to be put to trial in May 2005.

4 Trialling electronic voting: evaluation of the social impact

On May the 8th, 2005, elections took place throughout the province of Trento to choose town mayors and councillors: this turned out to be an excellent occasion to try on a large scale the electronic voting system that had been developed. Such an opportunity had no legal value, as electors were invited to test the new form of ballot after they cast the paper one, which remained the only valid one. The 7782 electors of the five towns chosen[2] for the field test received a letter of invitation and instructions: about 74% went to the polling station and cast the traditional paper-and-pencil ballot; of those, an average of 59% (with a peak of up to 80% in one of the smallest towns) tested the electronic system, too, and were asked to answer a questionnaire after completing the trial.

On the whole the participants were very satisfied with the system (Figure 3) although some problems were reported, especially in choosing councillors, in modifying a wrong choice, and in being sure that the procedure was terminated.

[2] according to a criterion based on their size and geographical location

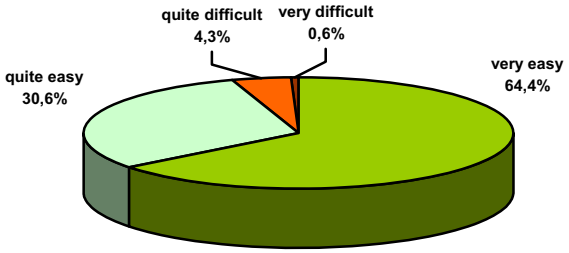


Figure 3: "How do you evaluate this new system of voting?" (%, *n*=5534)

Those who tested the electronic booth are a self-selected sample and it is reasonable to suppose that people who are very against e-voting were not among them. Nevertheless, the impression the participants got is altogether positive: 61% would be very favourable to voting only electronically already in the next provincial elections and only 10% would be very or quite against it, which is a remarkable result compared to that obtained before the field test took place (see Figure 2). The effect of exposure to different media on the perceived friendliness of the e-voting system was also considered and useful advice were taken up for the calibration of future communication campaigns. Last but not least, this field test revealed the importance of what we labelled as "scrutinizers effect", that is, the key role played by people at the polling station in reassuring and supporting electors, which leads to a higher turn-out in the electronic booth and a lower number of perceived impediments.

A second trial, on a much smaller scale, took place in November 2005 on the occasion of another round of local elections and provided a useful assessment of the modifications made to the system. Interestingly, in the town where this field test took place voter turn-out resulted in one of the highest in a ten years span, thus suggesting that electronic voting and the communication campaign that preceded it caused some kind of "Hawthorne effect" stimulating the citizens' curiosity and interest in elections. 89% of those who cast their ballot repeated their vote electronically (vs. 59% in May): though the absolute numbers of citizens involved in the two tests are very different (336 in November and 6950 in May), it is quite clear that greater attention to communication and to motivating scrutinizers significantly increases the voters' will to try electronic voting.

Voters' subjective evaluation of the system was extremely positive: none judged it to be very difficult to use and only 2% described it as "quite difficult" (compare with Figure 3). Electors who experienced some kind of trouble while testing the system relied on the assistance of scrutinizers whose support from outside the voting booth helped them overcome difficulties and resulted in a positive evaluation of the trial[3]. As with the first test, the respondents are a self-selected sample, which leads to an optimistic bias, but such a positive result indicates that the experience of using the touchscreen proved to be much easier than the image of it (as portrayed in Chart 2). The technical effort in improving the way councillors are chosen also abated the perceived hindrance in performing this operation, thus highlighting the importance of repeated tests and trials in "real world" settings to optimize the system according to actual voter-machine modes of interaction.

At present further studies are being carried out to test for the statistical significance of the trials on turn-out and on the vote cast, though from a strictly descriptive viewpoint electronic voting appears not to have impinged on attendance and the ballots electronically recorded are consistent with the paper ones, having legal standing.

5 Recalling memories: capitalising on the effects produced by the trials

A *post hoc* telephone survey on a sample of the citizens potentially involved in the first field test allowed us to further evaluate the social impact of the introduction of e-voting: recalling the memory of the elections some months after they took place helps to understand how much of this experience "remained". These follow-up interviews were aimed at monitoring the exposure to an array of media forms used during the communication campaign and to verify their effect on the decision of participating in the test. They also provided a useful assessment of the perceived trust in electronic voting: as Figure 4 shows, interviewees are altogether slightly more favourable to e-voting with respect to the first telephone interview (compare with Figure 2) and those who tried the electronic booth first hand are definitely very satisfied. Results for those who watched others e-voting are also reported, as well as the attitude of the citizens who declared not to have voted at all.

	sample	testers	watchers	non-voters
very in favour	**21%**	32%	12%	9%
in favour	**41%**	49%	39%	28%
indifferent	**17%**	8%	20%	36%
against	**14%**	9%	19%	12%
very against	**7%**	2%	10%	14%
N	***1206***	*503*	*372*	*146*

Figure 4: "Should electronic voting be adopted for the next provincial elections, would you be in favour or against this?"

[3] 61% of the interviewees answered to be *very in favour*, 26% to be *in favour*, 5% to be *against*, 2% to be *very against*, 6% to be *indifferent* to adopting electronic voting already for the next provincial elections (*n*=306).

Those who tested the touchscreen were also required to provide a subjective comparative evaluation of the traditional paper-and-pencil system and of the electronic one on a set of aspects such as user-friendliness, perceived secrecy, facility for interpretation of electors' will, proneness to vote tallying *et al.* The results show a preference for electronic voting regardless of sex, age, education and declared level of participation in elections. Consistently with the outcomes of the *pre-hoc* survey, favour towards electronic voting increases with level of education and participation and decreases with age, whereas paper-and-pencil balloting does not show any clear-cut trend related to these variables.

6 Conclusions

All through this paper we attempted to stress that studying social feasibility is a central issue in introducing such a substantial transformation as electronic voting. The impact of this innovation in a setting traditionally governed by symbolic and material customs is a very delicate matter that can be faced efficaciously only through the active involvement of all stakeholders: policy-makers, technologists, but above all citizens. We suggested a model of action research aimed at facilitating the switch from paper-and-pencil to electronic ballot, though further study is needed to provide a comprehensive assessment of the social impact. The results we presented suggest that citizens in the province of Trento are ready to accept the challenge but they need to be adequately supported by a communication campaign tailored to the needs of each social group. It is also important that more trials are conducted to help people get used to the new system before it is granted legal standing: only by "going local" and by listening to citizens it is possible to develop a voting machine truly compatible with their expectations and skills.

References

[Ed64] Edelman, M.: Symbolic Uses of Politics. University of Illinois Press, Urbana, 1964.

[Ke88] Kertzer, D.: Ritual Politics Power. Yale University Press, New Haven, 1988.

[Me02] Mercuri, R.: Explanation of voter-verified ballot systems. In ACM Software Engineering Notes (SIGSOFT) 27(5), 2002. Also at http://catless.ncl.ac.uk/Risks/22.17.html

[Se02] Servon, L.J.: Bridging the digital divide: technology, community, and public policy. Blackwell, Oxford, 2002

[SHB92] Shocket, P.A.; Heihberger, N.R.; Brown, C.: The effect of voting technology on voting behavior in a simulated multi-candidate city council election: a political experiment on ballot transparency. In Western Political Quarterly 45(2), 1992; S. 521-537

[Sl93] Slovic, P.: Perceived risk, trust and democracy. In Risk Analysis 13(6), 1993; S. 675-682

[TV03] Tomz, M.; Van Houweling, R.P.: How does voting equipment affect the race gap in voided ballots?. In American Journal of Political Science 47(1), 2003; S. 46-60

[Ve04] Venice Commission - European Commission for Democracy Through Law. Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe adopted by the Venice Commission at its 58th Plenary Session on the basis of a contribution by Mr. Cristoph Grabenwarter, 2004 http://venice.coe.int/

Session 8: Security for E-Voting

Security Requirements for Non-political Internet Voting

Grimm, Rüdiger[1]; Krimmer, Robert[2]; Meißner, Nils[3]; Reinhard, Kai[4];
Volkamer, Melanie[5]; Weinand, Marcel[6]; Helbach, Jörg[7]

[1]Universität Koblenz-Landau; [2]Wirtschaftsuniversität Wien; [3]PTB Berlin;
[4]Micromata Kassel; [5]DFKI Saarbrücken; [6]BSI Bonn; [7]GI Bonn
for further questions: grimm@uni-koblenz.de

Abstract: This paper describes the development of security requirements for non-political Internet voting. The practical background is our experience with the Internet voting within the Gesellschaft für Informatik (GI – Informatics Society) 2004 and 2005. The theoretical background is the international state-of-the-art of requirements about electronic voting, especially in Europe and in the US. A focus of this paper is on the user community driven standardization of security requirements by means of a Protection Profile of the international Common Criteria standard. An extended version of this article (20 pages) is published as technical report by the University in Koblenz (see reference list).

1 The GI and its election 2004

The Gesellschaft für Informatik (GI) is a society for computer science with presently about 24.000 members mainly from Germany. The rules for elections of the bodies of the GI are formally specified by the GI [GI03; GI04]. Since July 2003, the article 3.5.4 of the constitution of the GI allows the application of Internet voting. Here the precondition is that the Internet voting system provides the same security level as postal voting. In all cases where postal voting is admitted the election committee can decide to give members also the possibility to use an Internet voting system – as long as it is comparably secure. In summer 2004, the chairmanship (Präsidium) decided unanimously to offer both, postal voting and Internet voting for the chairmanship elections in December 2004. The election was successful. As a consequence the persons in charge decided to apply Internet voting again in 2005 for the election of the chairmanship and of the executive board of the GI. Until now the GI has voted online twice and plans to do so again in 2006.

After a market survey the GI chairpersons decided to use the POLYAS system [MM05] for Internet voting. The POLYAS system provides two authorization schemes, one based on authentication with digital signatures, the other employs PINs and user-ids instead. For better usability and simplicity, election PINs and personal user-ids were chosen for the GI election. Every GI member received a paper letter with the information material how to use the Internet voting system. In particular, the letter informed the member, that the user-id is the GI membership number. The PIN was printed on the letter and

concealed by an opaque (not transparent) sticker on the letter. The user-id and election PIN was used for registration. Finally, the letter specified the URL for the Internet voting system. Every voter who did not want to cast her vote electronically could alternatively participate by using postal voting.

The GI established a group of security experts to accompany the election and the future process of Internet voting in the GI. This group examined the specification and the documentation of the system, in particular with regard to data protection and manipulations. A main task of the expert group was to develop and enforce ad-hoc security requirements in cooperation with Micromata.

Micromata has done some minor changes on POLYAS to comply with the security requirements. Most security requirements could be met by organisational means. On a technical level, the following features were implemented

- audit proof archiving of the ballots preventing later manipulation of votes;
- separation of the electoral register from the ballot box; in particular, any shared marks were removed;
- SHA-signatures of software packages and result files.

Over 5000 members used the Internet voting system. The participation was significantly better than in several years before.

2 GI election 2005 – restructuring the security requirements

In December 2004, the Internet voting expert group of the GI decided to develop a requirements catalogue for „Internet-based elections in societies". They agreed on two preconditions. Firstly, the security requirements must ensure a security level not less than that of postal voting. Secondly, the catalogue should be short and crisp and should not exceed six printed pages. Four requirements catalogues were already available and could be used as a basis for further development: [CoE04; SCC04; PTB04]. After several iterations, a last version was published in [GI05].

The catalogue starts off with some preliminary notes and explicates assumptions under which any applied Internet voting system must ensure the security requirements. For example, it is assumed that the voter casts her ballot from an arbitrary Internet device connected to the Internet. Other assumptions are these: A non-secret name or a membership number (user-id) is applied for the voter identification. A secret alphanumeric password (one-time election PIN) is used for the voter authentication. The electronic ballot box and the electronic election register are installed on different servers. The two servers are located in different organisations. Postal voting is possible for every voter who does not want to cast an electronic ballot. The preliminary notes also define issues which are out-of-scope of the security requirements catalogue. For example, the candidate nomination and the maintenance of the list of eligible voters are not considered in the catalogue. Rules for a long-time storage of the election results are not addressed, either.

The catalogue of 2005 separates the requirements on the system development and on the election execution from those requirements on the Internet voting system itself. The requirements on the voting system itself are divided in requirements on the election servers and on the election software.

The general requirements on the system development contain requirements on the type and level of details of the system description, the security analysis and the manuals. There are especially strong requirements on the anonymity concepts. This category includes requirements on the development process, the system tests and the key management. The requirements on the election execution contain the distribution of the election PIN, the election register management and the installation as well as the de-installation of the voting system. The catalogue requires for the election servers to run a secure operating system, and to isolate the election software from all other applications. Only authorized persons may have access to the servers.

For the requirements on the election software the following categories were used.

- General requirements to an Internet voting system and its security
- Specific functional requirements to the Internet voting system
- Requirements with respect to the anonymity of votes
- Specific requirements to ensure a universal and equal election
- Ergonomic and usability requirements

The general functional requirements include the systems reliability and logging as well as the guarantee of consistent system states in case of any interruption. Specific functional requirements refer to the electronic register and to the electronic ballot box. Requirements with respect to the anonymity specify a secret, equal and universal election. The last category of requirements on the election software addresses ergonomics and usability.

3 GI election 2005 – meeting the requirements

On the basis of this agreed catalogue of requirements, Micromata was requested to explain how the POLYAS system ensures each of the requirements. Micromata has developed a new major release called POLYAS 2005 complying with the new catalogue of requirements. The main issues were:

- separation of the two servers, the ballot box and the election register;
- creation of a third server instance called the validator: the validator signs every entry of the electoral register before the elections starts; during the voting process the validator checks this signature of every voter from the register before it enables the voter to cast his ballot;
- system recovery, e. g. after system errors or client aborts during the election;
- detection of manipulations without violating the confidentiality of the ballots;
- several mechanisms to minimize possible system attacks by both, external Internet users and internal corrupted administrators: e.g. a check sum of each vote, the storage of votes as readable text and not as a database reference, splitting up the keys in a passphrase and a secret key to support the four-eyes-principle, firewalls and a „secure" operating system.
- documentation of all technical and organisational solutions to accomplish the security requirements;
- anonymous creation of the voters' PINs for the print service provider.

The technical solutions concerning error handling, recovery mechanisms, manipulation and threat scenarios were documented in detail. Organisational security solutions are based on the four-eyes–principle. At least two different persons must cooperate for administration of the systems, for starting the election application etc. The roles and responsibilities of the actors (management, administrators, voters, service providers etc.) are clearly specified in the documentation.

By applying the POLYAS system to the requirements catalogues we found out that several terms were used inconsistently. Thus, we developed a glossary including the terms election voting system, election voting software, ballot box, ballot box server, and authentication token.

Workshops in Kassel (home of Micromata) and Munich (home of one of the GI board members) revealed four new challenges:

1. Source code inspection: In order to increase trust in the decency of the software, and especially in order to identify undetected errors, Micromata and the GI expert group invited external experts to inspect the code of the POLYAS system. The inspection was not formal. Different experts of the GI community and of the Physikalisch-Technische

Bundesanstalt (PTB) inspected parts of the code on their own choice and on the background of their personal engineering experience. The code proved to be well structured. However, a set of improvements were initiated.

2. A simplified voters' guide [GIFS05]: The GI expert group specified a set of guidelines for online voters, which contains one page of general hints and thirteen easy-to-follow one-sentence rules for voters. The guidelines do not provide the illusion of a 100 percent secure client (which does not exist), but helps users to better assess their security level and to improve it on their own responsibility.

3. CC standardization of the requirements catalogue: In order to standardize the findings on security requirements the Common Criteria (CC) is the suitable framework. The GI expert group founded a sub-group to specify a CC protection profile for the security requirements of Internet voting for private societies and other non-governmental organisations. The GI would be one application field of the protection profile. This issue is discussed in chapters 5 and 6 of this paper in more detail.

4. A suitable comparison of Internet voting with postal voting: Despite the regulation of the GI elections that the security of Internet voting must be at least on the level of postal voting, these two voting methods cannot be compared in every respect. There are pros and cons with both systems, and in some respect, Internet voting is even much more secure than postal voting. For example an Internet voting system has the possibility to send an acknowledgement to the voter which informs the voter that her ballot has been stored. With postal voting the voter cannot know exactly if or if not her ballot arrives at the electoral office in time or if it arrives at all. The enforcement of anonymity is another advantage of Internet voting. Electronic ballots can be encrypted safely. Within postal voting, in contrast, it is much easier to open the well marked election letters. For a deeper discussion of this issue see [KrVo05].

4 The future of GI elections

The GI elections 2005 were a success, too. The participation was kept on the same improved level as 2004. There were no serious security attacks.

One problem was that the stickers on the paper letters were not as opaque as they should have been: very strong light was able to make the covered PINs visible. This is not a problem of the electronic system, but of the organizational implementation of the system. Another general problem is that a voting system must be able to handle differences between the number of voters that are registered as having voted and the number of votes in the ballot box. This may happen when messages between the servers get lost. The Polyas system offers protocol security mechanisms to detect such inconsistencies and fix them dynamically.

Plans for the next major release 2006 are:

- further improvement of the Internet voting protocol for a better system recovery after system failures;
- as an extension of the four-eyes-principle: implementation of an m-n threshold scheme for key distribution;
- support of EML (election markup language) for an easier configuration management;
- modified modules will help local chairs of GI subsections to administer their own elections.

Long term plans include the implementation of a rich voting client using bulletin board systems technologies. Rich voting clients allow for the implementation of security anchors in the hand of the voters.

As a consequence from this encouraging experience, the GI will continue to offer Internet voting to its members. Especially for the departments and working groups of the GI, Internet voting will be cheap, safe, and easy, and it will include much more members to execute their democratic right to elect their chairpersons.

5 International and European standards for e-voting

Discussions about the security of e-voting systems have often been led in a very emotional way. Following the falsification principle of Karl Popper the security of an e-voting system can never be proved but only perceived secure until proven otherwise. This, and the fact that anonymity in electronic processes is not an easy task, has led to numerous reports about erroneous and fraudulent e-voting systems. In order to reach confidence of the voters, developers and election operators have soon started to develop requirement documents which have often emerged to real standards. Note that electronic voting comprises the usage of voting machines and remote e-voting systems.

Germany was one of the first to have legal regulations concerning the use and testing of mechanical voting machines. The „Regulation of voting machines" [DE75; DE99] was set into place as a law on voting machines in 1975 and was changed in 1999 to allow for electronic voting machines. Currently only e-voting machines built by Nedap have passed the official tests by the German test authority PTB. These machines had been in discussion in Ireland for the national elections 2004. They are in use in several locations all over Germany. In the United States the use of voting machines is decided on a district level which makes national standards on those machines hard to push. Still the IEEE made an effort with the „Project 1583" [IEEE05] to develop such a standard in the aftermath of the 2000 Florida experiences. After a controversial debate about the draft standard, it finally was turned down and the working group is still trying to deliberate on the controversial issues.

For remote electronic voting one of the first discussions around requirements was the working group set up by US President Clinton in 2000 [IPI01]. It took place during the Arizona Primaries which was the first political election to feature e-voting for participation by the general public. The report of this working group defined a number of quality criteria for remote e-voting software to be met for a successful usage. In the succession of the Arizona experiment another project evolved: the election mark-up language standard. This has been developed by companies engaged in e-voting under the umbrella of the standardization organisation [EML05]. In Germany the national metrology institute PTB developed a criteria catalogue for networked polling stations in order to support the W.I.E.N. project. [PTB 04]. It uses a similar methodology like the one used for voting machines. This catalogue may serve as a basis for evaluation of Internet voting systems in Germany.

The largest effort to come to a common understanding by a set of criteria for both, remote electronic voting and voting machines, has been conducted by the Council of Europe [CoE04]. With the help of delegates from all 48 member states it has developed a set of legal, operational and technical standards on electronic voting. It is the most comprehensive and universal standard to date.

There are even many more collections of requirements with different foci. Nevertheless hardly any of the e-voting systems have ever been checked with reference to an international standard. The perceived security of the systems is most often based on some kind of an independent audit by experts. This lack of transparency can only be improved by proper documentation in the framework of an internationally accepted standard.

6 The CC approach of protection profiles

The Common Criteria (CC) is an international standard (ISO 15408) for computer security. The official name is „The Common Criteria for Information Technology Security Evaluation". Its purpose is to allow users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims. Thus, the CC distinguishes three groups: the customer, the developer and the evaluator. Independent of these three groups a certification authority certifies the related statements.

The Common Criteria results from a standardization of national security criteria from different sources, starting with the „Orange Book" of the US DoD 1985. The criteria are improved continually. At the moment the official Common Criteria version is the version V2.3. Today many nations (e.g. Germany, France, UK) have introduced the Common Criteria to define and certify IT security products and procedures. There is a growing list of nations which at least accept the CC-certificates (e.g. Spain, Greece, Italy).

The CC contains three parts: the Introduction and Common Model (part 1), the Security Functional Requirements (part 2), and the Security Assurance Requirements (part 3):

There is also a related document, the „Common Evaluation Methodology“ (CEM). The CEM guides an evaluator in applying the CC. They convert the assurance requirements of the CC to concret verification tasks. The CC defines two most important document types: the Protection Profile document (PP), and the Security Target document (ST).

A PP is a set of security requirements for a category of possible products, so-called Targets of Evaluation (TOE) that meet specific consumer needs. The requirements are independent of technical solutions, that is, PPs leave the technical implementation open. A PP distinguishes between security functional requirements and security assurance requirements, described in a very specific (semiformal) way defined by the CC. In addition there is a description part which describes the security concepts and the threats. In particular the description part maps requirements to the threats.

An ST document is to be created by a system developer, who identifies the security capabilities of his/her particular product. An ST may claim to implement zero or more PPs.

Both PPs and STs can go through a formal evaluation. The evaluation is done by an accredited laboratory. An evaluation of a Protection Profile is a pure document check. It simply ensures that the PP meets various syntactical and documentation rules as well as sanity checks. Therefore the evaluator has to check whether the set of requirements is exhaustive and self-contained. Successfully evaluated PPs are accredited by the German Federal Office of Information Security (BSI). Certificates for protection profiles are recognized and published internationally on the Common Criteria Portal.

A Security Target, in contrast, compares a concrete product with an ST document. The purpose of an ST evaluation is to ensure that the actual product (the TOE) meets the security functional requirements described in the Security Target. An ST can be based on one or more Protection Profiles if all included PPs are evaluated and if they have received a certificate of compliance. The evaluation insensitivity of the related TOE depends on the Evaluation Assurance Level (EAL), fixed as a minimum level in the ST or PP. The CCs predefine seven test depths (EALs) whereby Level 1 is the lowest and Level 7 the highest level. Level 4 is the highest level for typical commercial products and includes the source code evaluation. From level 5 and higher we need more and more formal specification documents.

A Protection Profile contains seven main parts: the Introduction, the TOE Description, the Security Environment, the Security Objectives, the Security Requirements, the Application Notes and the Rationales. A PP starts with the introduction part which contains document management and overview information. This part should help a potential user of the PP to determine whether the PP is of interest or not. The TOE description provides context for the evaluation to improve the understanding of the security requirements. The statement of TOE security environment shall describe the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed, i.e. assumptions about the environment, threats, and organisational security policies OSP (the OSP cover all regulations or laws which have to be supported by the TOE) . The statement of security objectives are

deduced from the security environment. The security requirements part of the PP defines the detailed IT security requirements to be satisfied by the TOE or its environment. The security requirements are the text blocks predefined in the CC-catalogue. The application notes are optional. They may contain additional supporting information about the construction, evaluation, or use of the TOE. The rationales part of the PP presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. This is a self check chapter for the PP editor.

The CC is a tool to build standard documents. The evaluated and certificated Protection Profiles are registered, available and accepted on an international level. The PP concept offers the customers the possibility to define their security requirements and standards for products. Thus, product developers are able to implement products that meet the customers' needs.

7 Summary and Conclusions

Internet voting has to guarantee the anonymity of voters and the authenticity of their votes. These two security requirements seem to be contradictory, but in fact they are not. Early solutions by homomorphic cryptographic functions or blind signatures have fascinated the academic community. However, related solutions were not accepted by a broad user community. Therefore, the German „Gesellschaft für Informatik" (GI) has decided to learn from earlier experiences and to try out a simpler version of Internet voting. In order to make this project serious, the GI – together with a professional system provider – developed an existing solution further and performed two elections electronically with the system while it was developed.

Besides other measures to improve security and transparency like source code inspection and usage guidelines, a set of security requirements was formulated and refined by public and expert discussion. Voting principles are basically the same in all democratic societies of the world. Therefore, it makes sense to formulate the security requirements in a way that the international community can share the experience and take influence. A standardized way of security requirements created by a user community is given by the instrument of a Protection Profile of the Common Criteria [ISO99].

We have initiated a working group to work on such a Protection Profile. Realistic applications are groups which have a need for decisions but do not often meet physically. Examples in the academic community are IFIP technical committees and working groups, IETF and W3C committees, and distributed project teams. In the economic life staff and workers councils and shareholder groups could profit from Internet voting. We expect a first published version of a Protection Profile for non-political Internet voting by late summer 2006.

References

[CC99] Common Criteria, Security Evaluation. Version 2.1, August 1999. ISO/IEC 15408:1999. And Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999. www.bsi.bund.de/cc/. See also www.commoncriteriaportal.org [6.4.2006]

[CoE04] Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Straßburg, 2004. http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf [6.4.2006]

[DE75] Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland („Regulation of voting machines for elections of the German and European parliament"), 03-09-1975

[DE99] Update 1999 of Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, Last update 20. 4.1999, http://bundesrecht.juris.de/bundesrecht/bwahlgv/ [6.4.2006]

[EML05] OASIS: Election Markup Language v.4. Last modified: January 24, 2005. http://xml.coverpages.org/eml.html [6.4.2006]

[GI03] Satzung der GI („Constitution of GI"), Bonn, 2003-07-21. http://www.gi-ev.de/wir-ueber-uns/unsere-grundsaetze/satzung/ [download 06 Jan 2006].

[GI04] Wahlordnung der GI („Regulation of Voting for GI"), 2004-09-21, Bonn, http://www.gi-ev.de/wir-ueber-uns/leitung/wahlen-und-ordnungen/ [6.4.2006].

[GI05] GI-Anforderungen an Internetbasierte Vereinswahlen („GI requirements for Internet based elections in non-governmental organisations"). 4. August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf [6.4.2006]

[GIFS05] Gesellschaft für Informatik and F-Secure Deutschland: Information für GI-Mitglieder zu möglichen Sicherheitsproblemen auf Clientseite bei Vorstands- und Präsidiumswahlen mit dem Online-Wahlverfahren. („Information about possible security problems for clients of online-voting"), 2005.

[Grim06] Grimm et al. (2006): Security Requirements for Non-political Internet Voting. An extended version (20 pages) of this article is published as technical report by the Institute for Information Systems Research of the University in Koblenz. 2006. http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGGrimm/Downloads [21.4.2006]

[IPI01] Internet Policy Institute (2001): Report on the National Workshop on Internet Voting, Issues and Research Agenda. March 2001. http://news.findlaw.com/hdocs/docs/election2000/nsfe-voterprt.pdf [6.4.2006]

[KrVo05] Krimmer, R.; and Volkamer, M.: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In EGOV (Workshops and Posters), 2005. 225-232.

[MM05] Polyas Online Voting Solutions – Online-Wahlen für Verbände und Vereine. Kassel. http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf [6.4.2006]

[PTB04] Physikalisch-Technische Bundesanstalt (PTB, 2004): Online Voting Systems for Nonparliamentary Elections – Catalogue of Requirements. Technical Paper PTB-8.5-2004-1, Berlin, April 2004. http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf [6.4.2006]

[SCC05] IEEE Standards Coordinating Committee 38 (SCC 38, 2005): Voting Standards. Project 1583 – Voting Equipment Standard; and Project 1622 – Electronic Data Interchange. http://grouper.ieee.org/groups/scc38/index.htm [6.4.2006]

Online Voting Project – New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles

Klaus Diehl, Sonja Weddeling

T-Systems Enterprise Services GmbH
Onlinevoting
Pfnorstr. 1
64293, Darmstadt, Germany
{klaus.diehl | sonja.weddeling}@t-system.com

Abstract: For several years, T-Systems Enterprise Services GmbH has been researching the creation of a highly secure voting system that meets the latest cryptological standards. With exclusive responsibility for the W.I.E.N (Wählen in elektronischen Netzwerken, Voting in electronic networks) research project supported by the government since 2005, T-Systems are studying the implementation of online voting in non-parliamentary elections. The voting system previously designed in this project was subjected to a thorough review by a renowned cryptologist from a German university in the summer of 2005. Some encryption processes were then modified, resulting in a highly secure voting protocol with the provisional working title of t-voting, which is simpler and quicker to implement. By adding important new steps within the core architecture, the strenuously disputed claims to the publicness of voting and its transparency are demonstrated. A public notice displayed on the bulletin board gives voters an overview of votes cast. Considering that online voting is seen as an alternative to postal voting, this actually increases the element of being "public". The principle of universality is augmented in online voting as the access options are simplified, which means that more voters can participate in the election.

1 Introduction

Since 2001, T-Systems has been researching the creation of a highly secure voting system that is virtually fraud- and interference-proof from cryptological perspectives with the assistance of the PTB (*Physikalisch Technische Bundesanstalt* - national metrology institute providing scientific and technical services) and other prominent institutes. T-Systems has been exclusively responsible for the W.I.E.N (*Wählen in elektronischen Netzwerken*, Voting in electronic networks) research project supported by the Federal Ministry of Economics and Labour since the start of 2005. This project involved the implementation of online voting at networked polling stations in non-parliamentary elections and its examination from a legal, technical and organizational viewpoint. During this project, past experiences in the field of electronic voting were

documented. In fall of last year, the voting system developed in the W.I.E.N. project using renowned cryptologists underwent a security review. The scientists came to the conclusion that the workflow of the core architecture was too laborious in various places and also contained security flaws. After a report was produced, the voting system was extended to include important cryptological add-on modules and the client-server architecture optimized. The result is a modified voting system core that incorporates state-of-the-art technical security and has been co-developed by the PTB. The environment of the voting system, which affects voting preparation, implementation and post-processing, has remained unchanged, as has the credo of an information-based division of powers and the use of blind signatures. The voting system being developed by W.I.E.N. was completed at the start of 2006, thereby concluding the project.

The newly developed and implemented voting system should now undergo a certification process based on the common criteria as per the ISO/IEC 15048 standard in cooperation with an accredited testing centre and the BSI (*Bundesamt für Sicherheit in der Informationstechnik,* Federal Office for Information Security). It is initially planned to create the protection profile, which is subdivided into three individual protection profiles relating to voting preparation, implementation and post-processing. The legislative instances for non-parliamentary elections in particular, e.g. work council elections, staff council elections and social security elections should be integrated early on. Once these protection profiles are created, they should be certified by the BSI to form the basis for their registration. When this process has been concluded successfully, an evaluation of the system in view of the previously established requirements is planned. Lastly, the voting system should be certified on the basis of the common criteria and also be subject to a comprehensive check by the PTB simultaneously to create a basis for legal legitimization.

In addition, the voting system developed in W.I.E.N., which is limited to the voting of networked polling stations, was and is being extended to include a remote voting system. The security requirements of such a system should first be examined and defined, and based on the results obtained software engineering should be the next step. The online voting project will perform business management studies of remote voting and the creation of its legal basis in parallel.

2 Adherence to Voting Legislation Principles

2.1 Voting legislation principles for publicly regulated elections with emphasis on the publicness of the election

For the analysis of the legal principles of elections, the voting legislation principles of Art. 38 of the Constitution of Federal Republic of Germany, federal, state and municipal voting laws and regulations for non-political elections (staff council, social security and works council elections) must be applied. The first principle is that of **universality**, in which the electronic voting must be equated to postal voting. A general election is one in which all citizens can participate regardless of their status or gender, and no voters are

excluded from voting unwarrantedly. Through improved access options such as e.g. the remote voting procedure which take account of the increased mobility and individualization of voters, the principle of universality is increased. The next principle is that of **directness**, which means that all entitled voters – without the interposition of electors - must cast their vote in the polling station themselves. There must be no further contact between voters and electoral candidates after voting. This voting principle generally poses no problems for Internet voting. Another principle is **freedom** of election, which means no pressure of any kind can be exerted on the voters, such as bans, sanctions or discrimination, to force them to participate in the election or to cast their vote for a specific party. Freedom of election is protected by the principle of confidentiality. The principle of freedom also includes permitting the possibility of casting an intentionally invalid vote. Next is the principle of **equality**, which means that all voters have the same number of votes with the same count and success value. The last principle refers to the **secrecy** of election. All voters must be able to cast their vote such that no-one can determine how they are voting or have voted. Voters must therefore be unobserved while casting their vote. In addition to the voting legislation principles expressly mentioned in Art. 38 I of the Constitution, there are unwritten constitutional voting principles, for political elections at any rate: publicness of election, simultaneity, comprehensibility and freedom of charge. The **publicness** of the voting process including the monitoring of the voting result is one of the most important tools for adhering to the principle of liberty. Publicness permits transparency and monitoring in elections and is necessary for all voting stages. This begins with voting preparations: polling dates and locations are publicized, the parties present their candidates publicly, electoral registers are displayed publicly and polling stations are made publicly accessible. Voting itself is a public act, but the casting of votes is secret. Finally, the determination of the election result and its publicization are also public. Votes are counted by the members of the electoral committee at a public meeting. The process of obtaining the voting result of both votes cast in person and the postal vote must be traceable for all citizens. Publicness must therefore also apply to the determination of the result.[1] Public monitoring is performed by the electoral committee, but also by any member of the public who attends. Remote Internet voting from a computer at home removes the location of voting from public view and should therefore primarily be used only as an addition to voting at the polling station.

The principle of **comprehensibility** of an election means that the act of voting must generally be simple and traceable for voters. If voting machines are used, the electoral committee must be provided with as much training material and technical expertise to allow it to guarantee and monitor the correctness of the voting process, which is its duty. Voters must also examine the casting of votes using voting machines.

[1] [KA04], p. 29.

Another point is the **simultaneity** of voting, which is still strenuously disputed in postal voting. There is a distinct advantage to Internet voting here, as in comparison to postal voting, which is generally a pre-vote, this permits the simultaneity of votes cast in person and remote voting.[2] Lastly, **freedom of charge** of election is an element of the democratic principle – voters must not incur a cost through exercising their democratic right to vote.

2.2 The new voting system and voting legislation principles

Public monitoring of digital voting both in person and remotely is problematic. From constitutional perspectives, the replacement of visual and comprehension monitoring by electoral boards and other members of the public (as witnesses etc.) is not possible.[3]

The voting system developed previously in the W.I.E.N. research project conformed to the principles of the Federal Electoral Law, which was implemented through the information-based division of powers and the use of reliable voter identification via a qualified digital signature.[4] By adding the bulletin board in the modified voting protocol, the strenuously disputed claims to publicness of election and its transparency can now be demonstrated. A public notice displayed using the bulletin board gives voters an overview of votes cast and can track voting live on the Internet if the electoral organizer wishes. Considering that online voting is seen as an alternative to postal voting, this actually increases the element of publicness. The principle of universality is increased in online voting as the access options are simplified, which means that more voters, including e.g. those impeded due to professional or health reasons, can participate in the election.

The public must be able to monitor the correct implementation of the election at all times. For this reason, they have read access to all content on the bulletin board. Only the voter status is not visible here if voting policy precludes this, which is to be assumed. The bulletin board is a passive data memory. This means that it cannot record or establish any proprietary communications. In this context, the bulletin board is viewed more as an instance as it does not participate in the newly introduced T-Voting voting procedure like the other roles. The role of the bulletin board is to make all necessary information available for implementing the voting process, taking this entitlement and access concept into account. As with a bulletin board, the data can be either read or written here depending on the rights of participants. Due to the restrictive nature of this concept, it is not possible to subsequently modify data that has already been written.

The role of the public refers to e.g. the following groups of people in works council elections:

- Entitled voters
- Unions represented in the company, or the relevant union representatives
- Employers

---

[2] [KA04], p. 34.
[3] [KA04], p. 30
[4] [BB00], p. 4.

During the voting preparation phase, the public has the option of contesting the electoral register. The 'notice' of the electronic electoral register and the process for contesting the register are already regulated in the applicable electoral regulations of the Works Constitution Act. During the voting stage, the public have no access to the data on the bulletin board. The participation of the public in the vote counting process, which is subdivided in turn into the mixing of votes and the subsequent counting of votes, is possible. The vote result can be published via the bulletin board for the user group of the public role after the votes have been counted.[5]

Public participation in the physical counting of votes is not possible due to restrictions of the medium as the votes are tallied by a computer program. However, to perform the entire process of electronic vote counting with the involvement of the public, once the electronic ballot box is closed vote counting is introduced with the process of vote mixing and the subsequent counting of votes by projecting attendance and determining the result at the polling station.

3 Technical Modification of the Voting System

3.1 Previous Voting Protocol

The voting protocol devised previously in W.I.E.N. was based on the voting protocol developed in 1993 by Fujioka, Okamoto and Ohta entitled "A practical secret voting scheme for large scale elections"[6]. This voting system primarily entails the physical and administrative separation of the electoral register and electronic ballot box. Specifically, the W.I.E.N. voting system consisted of four server services which are each linked with a database for storing persistent data. The relevant data memories, which are relational databases in their basic structure, were:

Distributor The distributor is used as a server service for transmitting the electronic constituency data. Using this, voters can connect to the authorized electronic electoral register (Validator) and the assigned electronic ballot box (Psephor) via the voting clients

Mandator In an election with voter ID/voter passport as a form of identification, the Mandator is responsible for outputting the keys of the voter

Validator The Validator provides the electronic electoral register for a specific election. Voters can also use the server service to log into the electronic voting system. The electoral office server releases the voting documents (ballot slips). It also confirms the blind vote.

[5] [PO06], p. 12 ff.
[6] [FU93], p. 244-251.

Psephor The data model of the Psephor contains the electronic ballot box. It manages the encrypted electronic votes and releases the ballot record in counting mode.

Voting client The voting client is used to determine the identity of voters, display the ballot slip, control communications, conceal and reveal information, and cast votes.

The voting protocol propagates the use of a blind signature procedure and other cryptographic procedures that protect cast votes from manipulation and unauthorized viewing. This voting protocol is still based on an encryption using public and private codes. Online voters are uniquely identified using a qualified digital signature.

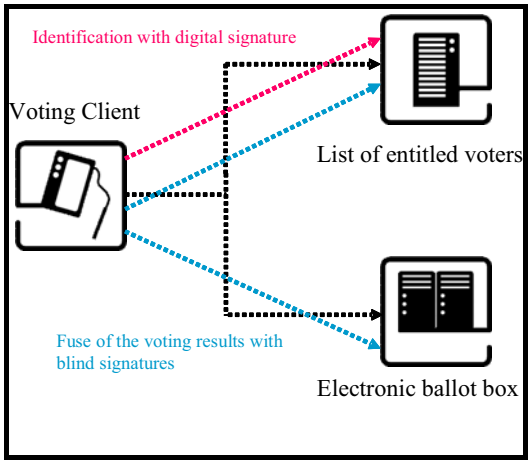


Figure 1: Principle of information-based division of powers

3.2 Newly implemented voting protocol

The voting system previously designed in this project was subjected to a thorough review by a renowned cryptologist from a German university in the summer of 2005. Some encryption processes were then modified, resulting in a highly secure voting protocol with the provisional working title of t-voting, which is simpler and easier to implement. However, the main principles of the previously developed architecture and the technologies used have remained the same.

The voter list server that issues voters with vote confirmation certificates using a blind signature[7] was also retained. Parts of the newly implemented cryptological techniques were examined back in spring 2005 using several voting tests and a legally valid test vote. In spring 2006, this voting system is also to be used for several works council elections and an Executive Staff Representation Committee election in the Deutsche Telekom group. Significant new developments include the addition of further participants. As a result, there is an interposed mix net, which separates the encrypted votes cast from the identity of the voter and stores these in random order. In addition, a bulletin board was integrated that acts as a bulletin board and shows the votes cast for everyone to see. Everyone can read messages published, but only authorized parties can store messages there. It is still not possible for anyone to delete or overwrite messages once they are written. Another element is the connection of a Tallier, which is responsible for counting the encrypted votes as a separate instance. All new developments were connected to the existing voting environment, including the administration modes.

[7] cf. [CH84]

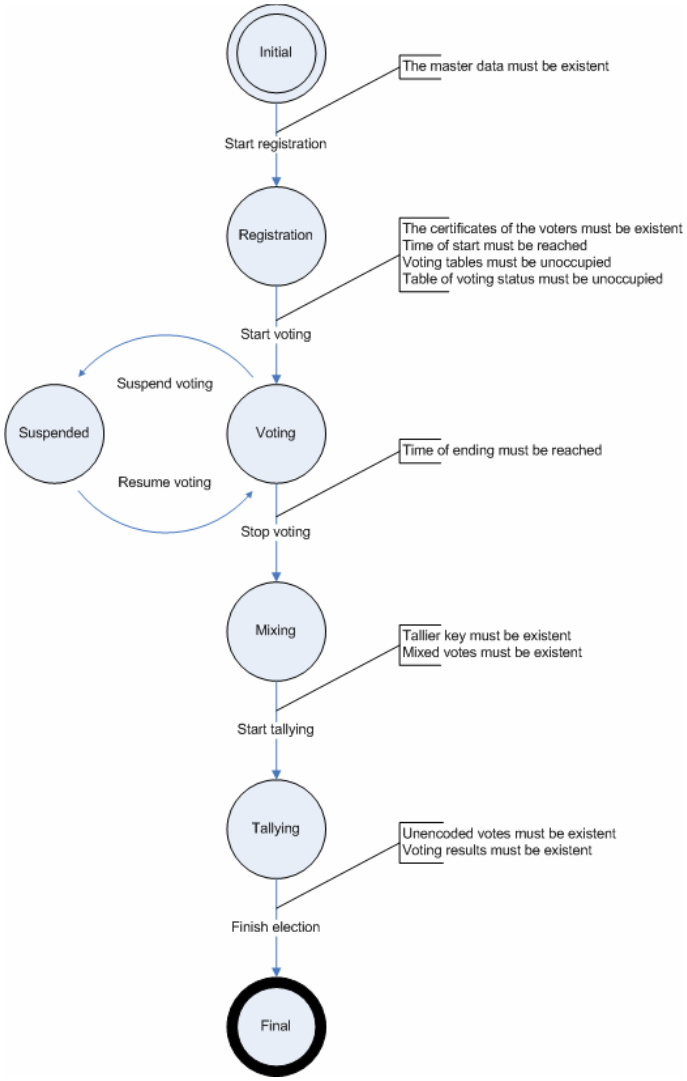


Figure 2: T-Voting phase model

The security requirements for electronic voting systems are not standardized, but science is agreed on a certain number of requirements:

Accuracy:

- A valid vote cannot be changed
- All valid votes are counted
- Invalid votes are not counted

Democracy:

- Only entitled voters can vote
- Each voter casts only one vote

Confidentiality:

- Anonymity: It is not possible to link a vote to a voter
- Untraceability: No voter can prove that he/she cast a specific vote
- A voter cannot be forced to cast a specific vote
- All votes remain secret up to the end of the election

Verifiability:

- Universal: Everyone can verify that all valid votes were counted
- Individual: All voters can verify that their valid vote was counted

The protocol uses blind signatures as per David Chaum. This mechanism prevents the signatory from being able to read the message to be signed. Another anonymization technique is the mix net as per David Chaum. Essentially, a mix net receives a number of messages, encrypts them and forwards the new messages in random order. The network thereby breaks the link between the incoming and outgoing messages. To ensure confidentiality and authentication, public key systems are used, e.g. RSA from Ron Rivest et al.

The system requires the following assumptions:

A trustworthy Public Key Infrastructure (PKI) is available and is used. All public keys are validated. A certification office issues relevant PKI certificates. This implies that all encryptions are performed using the correct public keys. All parties participate in the PKI. The cryptography used is strong and virtually unbreakable.

For communication, a protocol such as e.g. TCP/IP is used that secures the arrival of messages. We also assume that communication is protected by a protocol such as e.g. PKI-based TLS, which guarantees the reciprocal authentication of parties and the confidentiality of communications.

The registration stage is completed correctly.

There is trustworthy access control of the voting booth. This ensures that only entitled voters enter the booth, and that there is only one person in the booth at a time. The booth is constructed so that it is impossible to observe the voting process. This includes side-channel attacks (e.g. via power usage analysis).

The voting booth, mix net and bulletin board are considered trustworthy.

The voter, Validator and Tallier are not trustworthy. A valid vote is one that is in the correct form, is signed by the Validator, is encrypted in the correct order using the public key of the counter and the mix net, and is published on the bulletin board.

4 Conclusions

Through changes to the voting system developed previously in the Online Voting Project, most legal reservations against electronic voting were rebutted. The voting protocol became simpler and faster to implement, but most significantly now offers better integration of the general public through the use of a bulletin board. Previously existing technical security flaws were also eliminated. This brings us one step closer to our objective of making electronic voting feasible at networked polling stations in the short term and using any terminals without any technical, legal or organization problems in the medium to long term. We are assuming that online elections in non-parliamentary elections in Germany are now within the realms of possibility.

References

[BB00] Stephan Breidenbach and Alexander Blankenagel. Rechtliche Probleme von Internetwahlen. Berlin 2000.

[BU05] R. Araujo, A. Wiesmaier and Johannes Buchmann. The T-Vote Protocol. Darmstadt 2005.

[CH84] David Chaum. Blind signature system. In David Chaum, editor, Advances in cryptology: Proceedings of Crypto ’83, pages 153–156, New York, USA, 1984.

[FU93] Atsushi Fujioka, Tatsuaki Okamoto and Kazui Ohta. A practical secret voting scheme for large scale elections. In: Jennifer Seberry and Yuliang Zheng (Publisher) Advances in Cryptology - AUSCRYPT '92, Edition 718 der Lecture Notes in Computer Science, Page 244—251. Springer Verlag. Berlin 1993.

[KA04] Ulrich Karpen. Gutachtliche Stellungnahme zu elektronischen Wahlen. Hamburg 2004.

[PO06] Projekt Onlinewahlen, T-Systems Enterprise Services. Berechtigungs- and Zugriffskonzept Bulletin Board - Szenario: Betriebsratswahl. Darmstadt 2006.

[RI04] Volker Hartmann, Nils Meißner and Dieter Richter. Online-Wahlsysteme für nicht-parlamentarische Wahlen: Anforderungskatalog. Physikalisch Technische Bundesanstalt. Berlin 2004.

Session 9: Political Views and Democratic Challenges

The Voting Challenges in e-Cognocracy

Joan Josep Piles[1], José Luis Salazar[1], José Ruíz[1], José María Moreno-Jiménez[2]

[1]Grupo de Tecnología de las Comunicaciones
Universidad de Zaragoza
María de Luna, 1
50018, Zaragoza, España
{jpiles | jsalazar | jruiz}@unizar.es

[2]Grupo Decisión Multicriterio Zaragoza
Universidad de Zaragoza
Doctor Cerrada, 1-3
50005, Zaragoza, España
moreno@unizar.es

Abstract: e-Cognocracy[MP03, MP05, Ker03] is a new democratic system that focuses on the creation and social diffusion of the knowledge related with the scientific resolution of high complexity problems associated with public decision making. Using multicriteria decision making techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings, and the Internet as a communication support, e-cognocracy resolves some of the limitations of traditional democracy and provides room for greater involvement of the citizenry in their own government. In this sense, e-voting is not limited to the choice of a given political party, but to the extraction of the relevant knowledge.

Even though e-voting systems have already been widely studied, there are still some situations not covered yet by classical bibliography, and then it becomes necessary to introduce interesting variations to the main schema. In this paper, we will present one of such occurrences (that associated with e-cognocracy), and will study the modifications needed in the traditional e-voting processes as well as the implications they have.

1 Introduction

The degree of implication of citizens in their own government has traditionally been the issue which has led to most political changes throughout history. It has been traditionally agreed that it is desirable to achieve as much involvement as possible. This involvement should be only limited by what is practical for the smooth operation of the institutions.

This has been usually limited by the access of the citizenry to the relevant information, due to the lack of both education and readily access to the critical information. However, in the last years, with the advent of computers, the information flow between people has been steadily increasing. Internet is responsible for a great deal of this new communication, and it is being widely used by the very same citizens who will elect their leaders.

It is only natural, then, that technology has evolved to assimilate this new method of exchanging information into the classical structure. Thus, electronic voting, or e-voting, was born. However, there have been no shifts in the paradigm of the decission making process, although various different proposals have been made.

One of the obstacles these methods have is the lack of technologic means to allow their implementation. We introduce here one tool to allow one of these novel ideas, e-cognocracy, to be taken to reality.

In section 2 we will introduce e-cognocracy and its main differences with other e-voting schemes. Section 3 provides a description of our proposed voting system, as well as a proof that it satisfies the requeriments for its use in e-cognocracy. We offer in section 4 the details of our implementation and actual deployment of the system. Finally, in section 5 we provide the final considerations and future job within this project.

2 From e-democracy to e-cognocracy

Although Western societies have mainly opted for the "democracy" in their governance systems, in recent years there has been increasing discussion of a certain democratic fallacy, because this form of representation no longer meets its initial end, which is of course the participation of the citizens in their own government. Thus, many voices have been raised demanding greater involvement of the citizenry in the governance of society[Rob04]. One of the proposals suggested to improve this participation of citizens is e-cognocracy[MP03, MP05, Mor06]. It is a new democratic system employed to create a new, more open, transparent, civilized and free society that is at the same time more cohesive and connected, and more participative, equal and caring.

e-Cognocracy not only provides room for greater involvement of the citizenry in their own government and resolves some of the limitations of traditional democracy, but it also focuses on the process by which knowledge related with the scientific solution of problems is created and socialised. To this end, it uses multicriteria decision making techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings, and the Internet as a communication support.

Among the many tools needed to fully develop e-cognocracy, we will focus in e-voting, as it is the first needed to gather the information supplied by the citizens. Most known e-voting processes are limited to the technological aspects associated with the choice of a given party. However, e-cognocracy is focused on the extraction of the relevant knowledge, including the analysis of the individual and social learning derived from the scientific resolution of the problem, and this new orientation requires new technological features[Lot03, RH03].

From the point of view of the voting process, the key element introduced by e-cognocracy is the linkability of votes. In a traditional voting system, whenever the citizenry is asked to be part of a decision making process, a voting process begins.

This process starts with an information gathering phase. In it, each citizen is given the maximum amount possible of information from each of the interested parties (typically, political parties). This usually lasts for several weeks, in order to let every citizen get as much information as possible.

During that period there is very little feedback (if any) from the citizens who will partake in the votation. There are polls designed to get an idea of the actual tendencies, but they affects a very small percentage of the electorate. This, in turn, leads to a lost of interest, as the only really important moment is the voting itself.

In order to get the knowledge seeking process, we divide each votation in several rounds. Each voter can cast his vote in as many rounds as the voting process determines (but only once each round). After each round partial results are published, and more information is provided to the citizens.

For the actual results of the votation, only the last vote cast by a citizen is taken into account. However, all the history of different votations is preserved associated to the vote but not to the voter. This way, there is some information available about the trail each person followed until he arrived to his final decision.

Individual trails are never published, as they could compromise the secrecy of the voter. For instance one could be paid to vote first A, then B, then C and finally D. As the amount of rounds increases, the number of possible combinations becomes big enough to be relatively sure that only one person followed one given track. However, those trails give very valuable information which can help to detect the causes of the changes in opinion (e.g. not only that people switched from A to B, but also that most people switched after a certain event).

Also, people are encouraged to discuss their views in open forums, either anonymously or with an identity, and the effect of those discussions can be linked to the swings in the opinion of the voters.

2.1 Characteristics of our e-voting system

Our e-voting system is born as a tool for e-cognocracy and it has the following properties, sharing some of them with classic e-voting systems[BT94, CC96]:

Precision

- It shall not be able for a non authorized person to modify any votes (that is, only each voter can cast its vote).
- It shall not be possible to remove a valid vote from the final counting.
- It shall not be possible to include a non-valid vote in the final counting.

Democracy

- Only voters in the census shall be able to vote.
- Each voter shall be able to vote only once in each round.

Privacy

- A voter shall not be linked to its vote.
- A voter shall not be able to prove its vote.
- Verifiability
- Voters shall be able to verify that their vote has been correctly accounted.

Linkability

- Two votes from the same voter in different rounds of the voting shall be linked together, but not to the voter who cast them.

3 Our e-voting system

3.1 Actors in the voting process

Voter (V): Each voter must show its preferences in a multi-choice question, and rank them numerically. For each round of the voting the census shall be constant.

Certification Authority (CA): The Certification Authority shall issue the public/private keys and certificates for each actor involved in the process, and will serve as Trusted Third Party with regard to the validation of certificates.

Database server for the Electoral Authority (DBEA): The data shall be kept in a database in a secured location, without public access.

Recount server (R): The Recount server is the only entity allowed to decrypt the votes. The Electoral Authority shall provide information enough to link the votes from the same voter, but not to track them to the actual person who casted them.

Electoral Authority server (EA): The Electoral Authority shall keep track of the census, validate the users in the voting process, and sign their votes as a proof of voting. It shall also keep enough data about the votes to know the hash of the last vote from a voter (in order to link them for the Recount server) but without actually being able to decrypt them.

In this schema it is assumed that both the Electoral Authority and the Recount server do not work together to break the system and are trusted by each other and by the users. However, this is a reasonable assumption for most cases.

3.2 Initialization

The first part of the voting process is the initialization of the actors involved. In order to keep security, both the recount server and the electoral authority shall get a new key pair and certificate each voting. If desired, the keys for the voters can also be reset, though that's not necessary.

CA Initialization. The CA shall initialize only once before the start of any voting process. It shall do so by self-signing a certificate for itself and distributing it to the involved parties so that successive certificates may be trusted referring them to it.

R's private key initialization. The Recount server must decrypt all the casted votes with its private key. To avoid possible power abuses from a single owner of this key, it is possible to split it in different shares, so that a single person has not access to the voting data without coordination and acceptance.

EA's private key initialization. The Electoral Authority shall get a certificate and a key pair in order to do the blind signatures of each vote, which shall be kept by each voter as a proof of voting. It shall generate a census with the public keys of the persons allowed to vote.

Voters' registry. The Certificate Authority shall issue a new certificate and key pair to each voter who didn't have one yet, in order to be included in the census.

3.3 Voting

1. Voter makes his choices and saves the possible vote as a "voting intention" (this intention has no value as witness at all, as one could save as many of these "intentions" as desired without actually voting).

2. Voter encrypts the vote with R's public key.

3. Voter identifies himself to EA and sends it a hash of his vote for EA to issue a blind signature of it, and a ticket made from a mix of his identity and a random value that will be signed by EA as well.

4. EA verifies the voter's identity, checking it against the census and validating the client's certificate, and checks that the voter has not already cast its vote in this round.

5. EA issues a blind signature of the vote, and a signature of the ticket, and stores them linked to the voter for future rounds.

6. Voter sends to EA the vote and the blinding factor for the blind signature ciphered for R.

7. EA sends to R the ciphered vote and secret with the blind signature of it and the signature of the ticket via a secure channel.

8. If the voter had previously voted (in other rounds), EA sends to R a copy of the blind signature of the latest vote, which will be then used by R to link them.

9. EA sends to V the signature of the ticket to prove that his vote has been stored.

3.4 Recount

1. R makes public the signatures of the tickets, and starts a claims period before the publication of the results.

2. R decrypts the original votes, and uses the secret included with it to get a valid signature from the blind signature.

3. R checks the vote with the signature obtained and verifies that it is correct.

4. R links all the votes from the same voter.

5. R publishes the results of the round/voting.

3.5 Proof of fitness for e-cognocracy

In order to be used within the frame of e-cognocracy, our voting system must satisfy all the conditions previously imposed.

Precision

- As each voter authenticates himself to EA, this implies he must have a knowledge of the private key that is impossible to fake provided we use an adecuate key length.
- As each voter gets a signature of the ticket he sent to EA, and a list of those tickets is published prior to the recount, even if R is compromised, the votes cannot be erased from the ballot, as such an action would be challenged by the voters with their tickets, which would be shown to exist in EA.

- Each vote is stored with a signature from EA. A vote cannot be inserted even if R is compromised because it would be necessary to get a valid signature, and that is not possible without the private key of EA.

Democracy

- As the votes are not sent directly to R by the users, it is EA's job to get sure that the voter is properly included in the census.
- Analogously, EA will store which voters have already voted en each round, to avoid duplicates.

Privacy

- All the information provided to R is a ciphered vote, its blind signature, and a signed ticket. None of these includes anything that could lead to track the individual who casted the vote.
- The only item a voter receives is its signed ticket. That ticket is generated randomly, and has no relation whatsoever with the actual content of the vote.

Verifiability

- Each time a vote is received, EA sends back to the voter a signed ticket. Later, when the recount starts, the list of the tickets from the votes casted is published. If a voter had a ticket not included in the list, he could use it to challenge EA and see whether it has a copy of it. It EA has a copy, then the vote should be cast again.

Linkability

- Together with each vote, EA sends to R the blinded signature of the last vote casted by the same person. At the time of the recount, R looks for each vote the one which blind signature matches the included with the vote, and it reconstructs this way all the links which allow to trace the voting history of a voter, without actually revealing his identity.

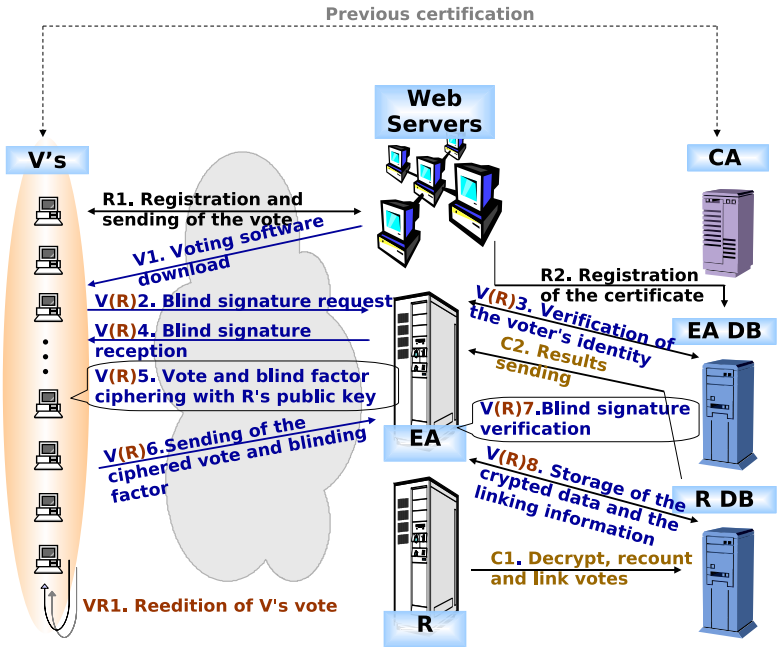


Figure 1: Overview

4 Implementation details

In order to implement the e-voting protocol, it has been chosen to use JAVA technologies, both in the client side and in the server side. This has several advantages:

- Better communication between the different components.
- More code reusability, as we can develop a series of cryptographic libraries which will be used both by the client and by the server software.
- Easy integration with the browsers.

In order to minimize the number of configurations in which the client side had to run, we decided to choose a standard web browser. In this case, it was selected Mozilla Firefox as the reference browser. It has the advantage of being open source, so its source code is readily available, contributing to increase the feeling of transparency in the process.

The browser has been completed with some libraries (JSS), needed to be able to access the client certificates which are stored in it from within the JAVA applet that will be the client software. If those libraries were not available, the user should manually add the client certificate and the CA to the JAVA application.

The application server to use will depend on the available infrastructure at the moment of the deployment. In our tests, we used Tomcat as application server. It is open source as well, and its capacity for this kind of systems is well proven.

It was chosen to use MySQL as a backend to store the data related to the votings (both the actual votes -ciphered and clear-text after the recount- and the information about the votings -question of the voting, number of rounds, period of time for each round...).

As there are two different servers (Electoral Authority server and Recount server), there could be two web and application servers, working with two different database servers. None the less, when doing the actual deployment it might happen that it is advisable to put both applications in the same application and/or web server. Likewise, it could be desirable to use two databases in a single database server. This would not be a problem, but it should be taken into account that should the server machine be compromised, the whole voting and recounting system would be broken.

All the communications between the client and the server will be both authenticated and encrypted. To achieve these goals, it will be necessary to set up an infrastructure allowing SSL and client side certificates.

4.1 Deployment details

Our group carried out a deployment of a test voting system. None the less, any future deployments should take into account that the specific details will depend on the available resources. This will be much more important if, as it usually happens, the servers are shared with other applications. The implications for the security of the system must be studied on a case by case basis.

Regarding the choice of software, we used Apache as the webserver and Tomcat 5 as application server, both of them running in LINUX i386 machines. As this was a proof of concept, the system load was expected to be very low. This allowed us to consolidate both services (the Certificate Authority server and the Recount server) within the same Tomcat instance. Likewise, both databases were stored in a single MYSQL server which was executing in the same machine with Apache and Tomcat.

There are several options available to link Apache and Tomcat. The simplest way is running two independent servers listening in different ports (in fact, it would even be possible to have them running in different machines, should the need arise). Notwithstanding this, we chose to use a tighter integration between them using the JK Connector. This technology allows to redirect queries that would normally be answered by the Apache server towards the Tomcat application server, in a way that is transparent for the user.

However, this choice makes the Tomcat application server unaware of the underlying SSL layer, because the web server forwards the request to the application server, but not the environment and security layer data. Even though the voting system cannot obtain the client certificate from the SSL layer, our protocol allows for the certificate to be sent by the client in case the server is not able to directly retrieve it.

In order to generate the certificates needed, we also set up a Certificate Authority using OpenSSL.

5 Conclusions

We have studied the novel challenges that e-cognocracy imposes upon traditional voting. We have built an e-voting system which provides the means to gather the information needed towards a more participative democracy.

As we have seen, the key to get the linkability of the votes is the separation between the Electoral Authority, who can link the chain of votes to the user but can't know the contents of each vote, and the Recount server, who can link the votes between themselves and decrypt them, but is isolated from the information about each voter.

This isn't a concern as long as both of them are trusted entities who will not work together to cheat the system.

We have also built and tested such a voting system, showing that it is feasible and that its ease of use allows for it to be widely used without any special kind of technical background.

Our future work includes developing other technological tools needed by e-cognocracy. As e-voting provides the raw data, there is still the need for a set of tools which can link the information obtained to the actual social phenomena that helps to form the results obtained in the votation. These tools includes online forum where people can exchange ideas in a controlled way, and the tools needed to extract the relevant or prevalent opinions and match them against the shifts in the voters' opinion.

6 Acknowledgements

This work has been partially funded under the research projects "Electronic Government. Internet-based Complex Decision Making: e-democracy and e-cognocracy" (Ref. PM2004-052) and "Internet-based Complex Decision Making. Decisional Tools for e-cognocracy" (Ref. TSI2005-02511).

References

[BT94] Benaloh, J. and Tuinstra, D. Receipt-free secret-ballot elections (extended abstract). In STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing, pp. 544–553. ACM Press, 1994.

[CC96] Cranor, L. F. and Cytron, R. K. Design and implementation of a practical security-conscious electronic polling system. Technical Report WUCS-96-02, Washington University, 1996.

[Ker03] Gregory E. Kersten, G.E. e-Democracy and participatory decision processes: lessons from e-negotiation experiments. Journal Multi-criteria Decision Analysis 12(2-3), 127-143, 2003.

[Lot03] Lotov, A. Internet tools for supporting of lay stakeholders in the framework of the democratic paradigm of environmental decision making. Journal Multi-criteria Decision Analysis 12(2-3), 145-162, 2003.

[MP03] Moreno-Jiménez, J. M. and Polasek, J. M. e-Democracy and knowledge. a multicriteria framework for the new democratic era. Journal of Multicriteria Decision Analysis, 12:pp. 163–176, 2003.

[MP05] Moreno-Jiménez, J. M. and Polasek, J. M. e-Cognocracy and the participation of immigrants in e-governance. In TED Conference on e-government 2005. Electronic democracy: The challenge ahead, volume 13 of Schriftenreihe Informatik, pp. 18–26. University Rudolf Trauner-Verlag, 2005.

[Mor06] Moreno-Jiménez, J.M. E-cognocracia: Nueva Sociedad, Nueva Democracia. Estudios de Economía Aplicada 24(1), 559-581, 2006

[RH03] Ríos Insúa, D., Holgado, J. and Moreno, R. Multicriteria e-Negotiation Systems for e-Democracy. Journal Multi-criteria Decision Analysis 12(2-3), 213-218, 2003.

[Rob04] Roberts, N. Public Deliberation in an Age of Direct Citizen Participation. The American Review of Public Administration, 34(4):pp. 315–353, 2004.

E-Voting in Slovenia: The view of parliamentary deputies

Tina Jukić, Mirko Vintar

Faculty of Administration
University of Ljubljana
Gosarjeva 5
1000, Ljubljana, Slovenia
tina.jukic@gmail.com, mirko.vintar@fu.uni-lj.si

Abstract: The paper presents the results of the research, focused on Slovenian parliamentary deputies' position on e-democracy with the stress on remote e-voting. It examines the difference in the position on e-democracy and e-voting of deputies aligned with the political right and left respectively. Furthermore, it considers deputies' attitude to the initiatives mediated via e-mail and assesses the risks and impact that the deputies see in e-voting. They were asked to what level they supported the implementation of e-voting and when, in their opinion, Slovenia would start e-voting tests. Finally the authors indicate the most interesting findings of the survey.

1 Introduction

There has been a great deal of discussion on e-voting over the last few years, especially within projects in Estonia, the United States, Canada, Spain, France, Switzerland, and the UK, among others. Optimists forecast greater elections turnout, pessimists warn about underdeveloped technology. The experience of other countries, which all the e-voting pioneers should take into account, is that a 'step-by-step' approach is best, which means that we should start by implementing e-voting in municipal elections, and perhaps not even in all of them.

Slovenia has not yet started any e-voting projects. An e-voting feasibility study was made in 2003, and e-voting amendments were proposed to the National Assembly Elections Act. But these amendments were not carried, which is the reason there is not yet a legislative basis that would enable this kind of voting.

Not knowing what the plans about future e-voting efforts are stimulated us to conduct a survey to find out the position of Slovenian parliamentary deputies on e-democracy with an emphasis on remote e-voting. Since the current ruling coalition consists mostly of right-aligned[1] deputies, and since, traditionally, the Right is more conservative we wanted to see, if we can expect further delays in e-voting progress. We carried out an e-mail survey, sent to all (90) deputies.

Most of regular internet users in Slovenia are among highly educated population (90%) [SO06], while, on the other side, the largest left-aligned party (Liberal Democracy of Slovenia) has more voters with higher education than the largest right-aligned party (Slovenian Democratic Party) [AP04]. This is the reason we started our survey with the hypothesis that the current ruling coalition is not in favour of e-voting, which could cause further postponement of e-voting.

The purpose of the paper is therefore to present the most interesting results, on the basis of which assumptions can be made about the further evolution of e-voting in Slovenia. First, the paper presents the current state of e-voting efforts and the research scheme. The next section presents the results of the survey and finally conclusions are drawn.

2 Presentation of the state

There is no legislative foundation to enable e-voting in Slovenia. The most important source of electoral law in Slovenia is the National Assembly Elections Act, with other electoral legislation based upon this Act. In 2003 some amendments to this Act were proposed, including e-voting, but this proposal was not supported by the Right in parliament, so the amended Act did not become law. Most of the arguments related to 'underdeveloped' technology [Ko04].

In July 2003 Government adopted a decree establishing a project council that was chaired by the Minister of the Information Society. The project group, established in December 2003, formed its first concrete guidelines for e-voting implementation in the first quarter of 2004. Three documents were prepared: (1) A scheme for a study on e-voting with a review of electoral procedures [MIS03], (2) The feasibility study: constitutional and political views on introducing of e-voting in the Republic of Slovenia [GLZ04], the Ministry of Information Society also produced a (3) Feasibility study of e-voting with the implementation proposals [Tu04]. One of the main finding of the second document was that "the use of ICT in electoral procedures is a welcome contribution to the democratization of the society." At the same time the study warned of negative effects caused by faults (e.g. technical, procedural, system) (ibidem). The review of electoral procedures for the execution of e-voting indicates that only three procedures (out of 33) exist in electronic form: (1) insight into data on right to vote, (2) electronic announcement of unofficial data and (3) electronic announcement of official data.

[1] Not all of political parties are extreme left/right-wing; we use the term left/right-aligned or simply Right/Left.

At the end of 2004 a new government took office. Its prime minister is also the president of the largest right-aligned political party. The new government abolished the Ministry of Information Society and the Government Centre for Informatics, with most of their tasks falling within the Directorate for E-Government and Administrative Processes. The current situation indicates that the e-voting project has stalled. Local elections in the present year could be a great opportunity for the e-voting pilot project, but it seems likely this will not occur. There are grounds to be anxious about e-voting projects and some other e-government projects.

It is worth mentioning that less than 10% of the Slovenian population has a digital certificate [Ce05] and the promotion of e-government services is at a low level. On the other hand, survey results [IT04] showed that 54% of respondents would participate in internet voting; it is interesting that there 58% of potential e-voters are internet users, while among non-users there are 36% of potential e-voters (ibidem).

The Strategy of E-Commerce in Public Administration of the Republic of Slovenia for 2001 to 2004 is out-of-date, so there is a vacuum[2] in the field of strategic planning of e-government, and we can only hope that the next Strategy will also include efforts to implement e-voting.

2.1 Other authors' findings

This section sets out some e-voting findings by other authors and other countries' experiences, on which our conclusions will be based.

Local e-voting. As Rivest [html1] assesses, local (county) level e-voting projects are better than national e-voting. This assessment has two arguments (ibidem): (1) there is no common point of vulnerability, which could be the target of attackers, (2) letting individual local levels of government experiment with different techniques is a good way to acquire experience.

Multiple voting. We think, that even though one of the fundamental principals of (e)-voting is 'one voter – one vote', Estonia [NEC04] makes good use of multiple voting – in the field of e-voting they consider multiple voting can prevent from vote-buying. The system only takes the last vote into consideration.

Turnout. Switzerland [So05] ascertained that internet has an impact on the group of voters aged 18 – 29 years; voters in this age group cast only 7% - 8% of all ballots, but when they had the possibility of e-voting, they cast 10% of all ballots. On the other hand, several authors think that e-voting should not be correlated to an increase of the turnout. The UK's Electoral Reform Society, for example, found that alternative voting methods (postal, SMS, internet, and digital TV) tested in local elections have not led to an increased voter turnout [ID03]. Furthermore, Norris [No02] drew a conclusion that 'e-voting would only have little or no effect on turnout'.

[2] The new strategy is in preparation.

Costs. Remmert [Re04] also sees one of the reasons for e-voting implementation in a gradual reduction of the cost. Furthermore, Van Den Besselaar et al. [VODF03] also sees a good argument for e-voting in lower costs – he finds that, in contrast to traditional voting, there are no additional costs if the e-ballots continue over more days.

3 Research methodology

The main goal of the research was to find out the deputies' position on e-democracy with an emphasis on the remote e-voting. The research was particularly focused on:

- deputies' familiarity with e-voting projects in other countries,
- their attitude to the initiatives, proposals and questions sent by e-mail,
- their opinion on e-voting effects,
- the risks they see in e-voting,
- levels at which they support e-voting implementation, and
- their assumptions on when Slovenia will start e-voting projects.

For this purpose we conducted a survey, sent by e-mail to all (90) deputies. The survey was sent on 16 January and we received 29 replies by 6 March, 16 of which came from the members of the Right[3] and 13 from the Left. Fifty-seven per cent of parliamentary deputies are aligned with the Right and 41% with the Left[4]. Figure 1 shows the percentage of members on the Right and Left and the percentage of replies:

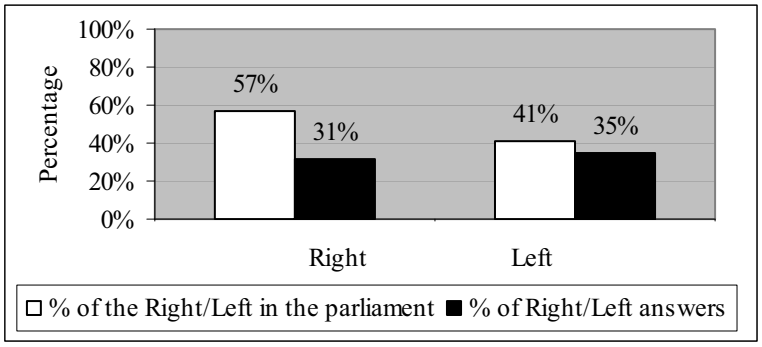


Figure 1: The percentage of the members of the Right and Left and the percentage of their answers
The percentage of returned polls is to low to generalize overall results, so there must be some reservation regarding the results.

[3] We consider that right-aligned parties to be the Slovenian Democratic Party, Slovenian National Party, Slovenian People's Party and New Slovenia, and that the left-aligned parties to be Liberal Democracy of Slovenia, Social Democrats and Democratic Party of Pensioners of Slovenia.
[4] Two representatives represent two minorities: Hungarian and Italian.

4 Presentation of the results

4.1 Familiarity with e-voting projects in other countries

As is known, some countries have already implemented e-voting in their electoral systems, while some have been implementing pilot projects for some time. We wanted to find out if Slovenian deputies were familiar with these projects.

The survey revealed that most of them (66%) had already heard something about these projects, but they were not familiar with all the details, while 14% of deputies receive information on other countries' e-voting projects on a regular basis, and 10% were not acquainted with these projects. A further 10% of them were acquainted only with the US and Estonian e-voting projects.

4.2 Attitude to the initiatives, proposals and questions mediated via e- mail

At this point we wanted to find out:

- if the deputies consider e-communication equivalent to traditional communication of proposals, initiatives and answers,
- how often they receive proposals, initiatives and questions via e-mail and
- how they treat proposals, initiatives and questions via e-mail.

The results are surprising – 48% of deputies consider e-communication equivalent to the traditional communication of proposals, initiatives and answers, while 48% of them thought that e-communication is only partly equivalent to traditional communication, and 3% thought that e-communication is not equal to traditional communication.

Most (66%) of deputies receive proposals, initiatives etc. via e-mail at least once a week, 21% of deputies receive them at least once a month, 10% receive them at least once every six months, while proposals etc. are never mediated via e-mail to 3% of deputies.

Interesting, almost half (48%) of deputies considered e-communication only partly equivalent to traditional communication, but when it comes to treatment of initiatives etc. sent via e-mail, 85%[5] of deputies say that they thoroughly studied the material and take it into consideration as much as possible. The results of the survey [De05] make our results even more interesting – in 2004 the deputies' response wasn't that high, 40% of them responded to the e-mail with a real case question from an imaginary citizen[6]. The question is, do 85% of deputies from our survey really study the initiatives, proposals etc. thoroughly? We think that this data should be taken into account with some reservations.

[5] n = 27
[6] In 14 days.

4.3 E-democracy and e-voting effects

The effects of e-voting were estimated on a scale of 1 to 5. The deputies assessed five parameters:

- citizens' e-participation influence on the quality of legislation and other decisions,
- e-voting effects on authority's legitimacy,
- e-voting effects on the turnout,
- e-voting effects on the movement in electoral body and
- the security of e-voting.

The survey revealed (Figure 2) that 66% of deputies thought that e-participation would influence the quality of legislation and other decisions – that was the opinion of 77% of the Left and 56% of the right-aligned deputies. Moreover, 28% of deputies thought that e-participation may or may not influence the quality of legislation – this is the opinion of 38% of the Right and only 15% of the left-aligned deputies. Interesting, most of the left-aligned deputies thought that e-participation would have influence, while this is the opinion of far fewer (56%) members of the Right:

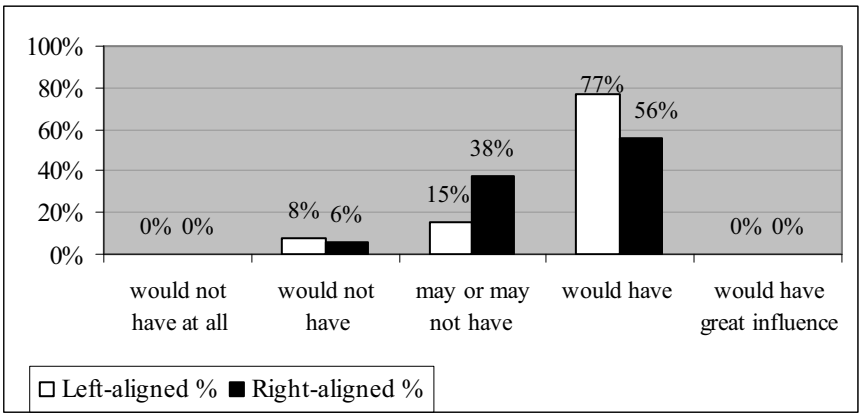


Figure 2: Citizens' e-participation influence on the quality of legislation and other decisions

Furthermore, the results show that there is a difference in Left/Right agreement with the statement "E-voting would contribute to a greater legitimacy of elected authority." Most of the right-aligned deputies (44%) disagree with this statement, while most of the leftists (46%) agree with it. On a scale of 1 to 5 the median for the Right is 2, while the median value of the Left is higher – 3.

The difference can also be seen after analysing the agreement with the statement "E-voting is secure" – most of the Right (50%) disagrees, while 42% of the Left agree and the same share neither agree nor disagree with this statement. On a scale of 1 to 5 the median of the Right is 2, and the median value of the Left is 3.

When it comes to the influence of e-voting on higher polling participation, the deputies are even more heterogeneous; most (50%) of the right-aligned deputies agree that e-voting would have influence on a higher turnout and most (85%) of the Left agree with this statement, too.

Most (69%) of the left-aligned deputies agree that e-voting would have influence on the movement in electoral body; on a scale of 1 to 5 the median of their agreement is 4. On the other side, most of the right-aligned members (44%) neither agree nor disagree with this statement; their agreement's median is 3.

If we neglect the Left and Right division and take a look at Figure 3, we can see that the situation is rather pessimistic. Most of the deputies (34%) disagree with the statement that e-voting would have an influence on the greater legitimacy of elected authority, only 28% of them agree and the same proportion (28%) neither agree nor disagree that e-voting is secure, while most of them (45%) agree with the statement "e-voting would have influence on the movement in electoral body."

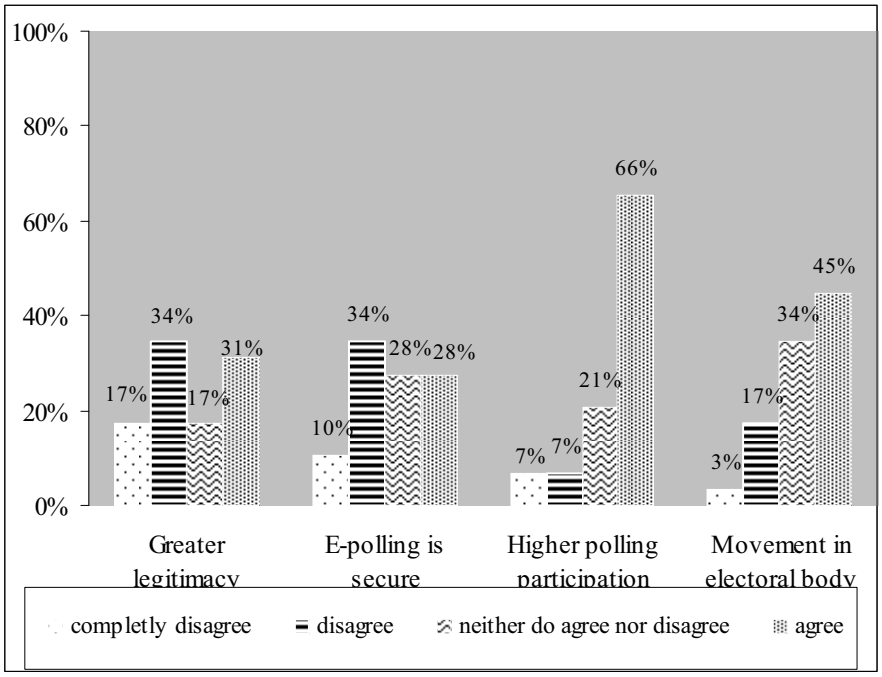


Figure 3: Deputies' views on e-voting effects[7]

There is one optimistic result – most of them (66%) agree that e-voting would have influence on higher polling participation (turnout).

[7] None of the representatives completely agreed with the statements listed above.

4.4 The reasons for Slovenia still not having a legislative basis for e-voting

We wanted to find out the main reasons for not having at least a legislative basis that would enable e-voting in Slovenia. The results[8] show that most (45%) of the deputies blame "underdeveloped" technology for the legislative "vacuum." Furthermore, 17% of deputies thought that the reason for not having a legal basis is the fear of some political parties that implementing e-voting would cause higher participation of younger and technologically more educated registered voters.

As may be seen from Figure 4, most (60%) of the right-aligned deputies blame the "underdeveloped" technology, while most (42%) of the left-aligned deputies blame the fear of some political parties, which are worried about higher turnout caused by e-voting.

Beside the reasons listed below (Figure 4), the respondents expressed some other reasons, such as (1) how would one assure that every voter had only one vote, (2) the risk that a voter could vote instead of other members of the family, (3) how to prevent people breaking into the e-voting system, (4) how to achieve voters' trust in e-voting, (5) bureaucratic reasons (formalities).

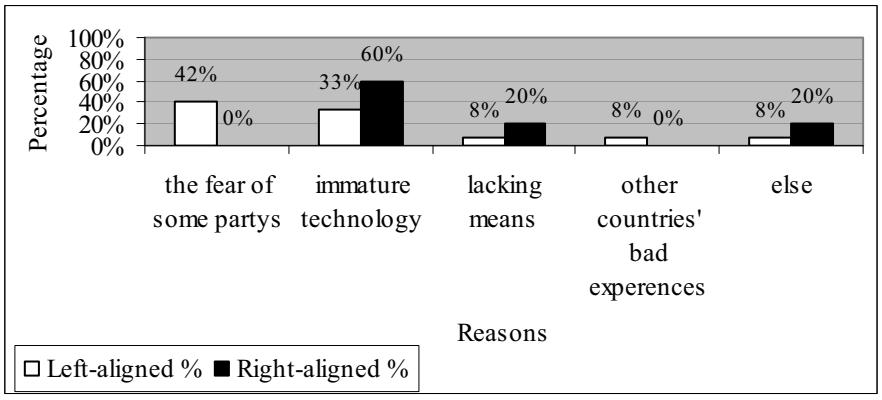


Figure 4: The reasons for not having a legal basis for e-voting

4.5 E-voting risks

We also asked the deputies which, in their opinion, are the greatest risks of e-voting. They were able to choose three answers at most.

[8] n = 27

The survey revealed that most of the respondents (66%) saw the biggest e-voting risk as the violation of some basic election principles: secrecy, freedom and (re)check. The lowest (24%) proportion of respondents was worried about double voting, and (28%) manipulation by the current ruling powers. Furthermore, 52% of deputies thought that excluding people who do not use the internet and those, who are not educated enough to e-vote is a threat to e-voting success, and 45% of them had doubts about system (collapse); 31% of deputies selected its possible influence on voter's decisions.

It is not surprising that, in contrast to the Right (13%), 46% of left-aligned deputies saw the main risk of e-voting as the possibility of manipulation by the current ruling powers.

5 The future of e-voting project in Slovenia

In this part we wanted to resolve two matters:

- to what level do the deputies support the implementation of e-voting (they were able to choose whichever level) and
- when, in their opinion, will Slovenia start testing e-voting.

The results show that most deputies (66%) support e-voting for national referendums, 48% of them support e-voting in the elections for president of the state, 48% support e-local referendums and 38% of respondents support e-elections of deputies. It is obvious that deputies are most sceptical about e-elections of themselves.

There is a significant difference in Left and Right support (Figure 5). As we can see, local e-referendums are supported by 69% of Left members, while only 31% of the Right members support this project. Moreover, 38% of Right members do not support any kind of e-voting, while all Left members support e-voting on at least some level listed.

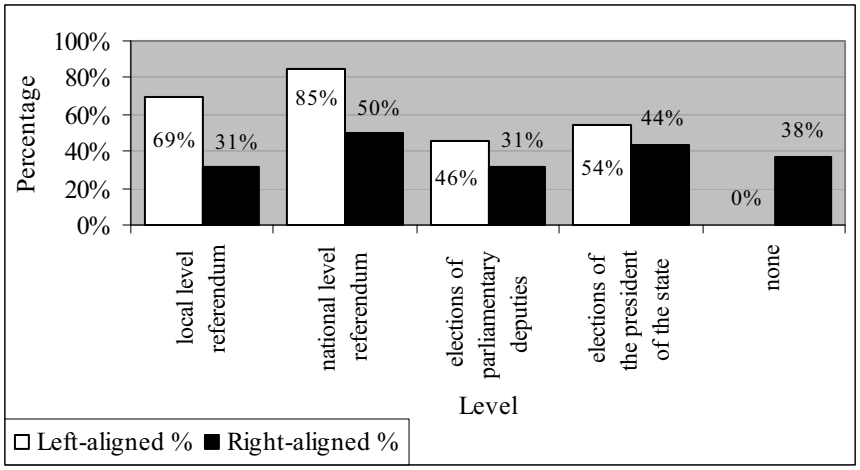


Figure 5: The levels on which Slovenian deputies support the implementation of e-voting

A total of 46%[9] of respondents thought that Slovenia will start e-voting test projects before 2010, among which were 62% of Left and 33% of right-aligned deputies, while 54% of respondents thought that e-voting projects would start after 2010 (38% of Left and 67% of Right).

5 Final remarks

The most interesting survey results can be summarized as follows:

- it is strange that only 14% of right-aligned members were well informed on other countries' e-voting projects, because the Right has been most responsible for delaying the amended law to enable e-voting. If they are not aware of others' countries e-voting projects in detail, than it is clear that their resistance to the amended Act was not based on professional arguments;

- some 48% of deputies thought that e-communication was only partly equivalent to traditional communication of proposals, initiatives, questions etc., but 85% of respondents said that they thoroughly study the initiatives etc., received via e-mail and take them into consideration as much as possible; on the other side, the survey [De05] revealed that deputies' response levels are not very high – 40% of them responded to a simple real case question from an imaginary citizen;

- the fact that 77% of the Left and only 56% of the right-aligned deputies thought that citizens' e-participation would influence the quality of legislation and other decisions is something to be anxious about, since the current ruling coalition consists primarily of right-aligned deputies;

- only 48% of respondents supported e-voting on the local level, which is interesting, since most of other countries started with e-voting projects on the local levels (municipalities); moreover, Rivest [html1] assesses, that local (county) level e-voting projects were more highly recommended than state e-voting (see section 2.1); it is possible that this answer is correlated to the forthcoming local elections in Slovenia; furthermore, it is interesting that the lowest proportion of respondents expressed support for the e-voting of deputies. If we look at these results critically, the message seems to be "e-vote for anyone, but not for us";

- some 21% of deputies neither agreed nor disagreed with the influence of e-voting on higher polling participation (turnout); this result is understandable, since the authors and other countries' experiences are not united on this question, either (see section 2.1);

[9] n = 28

- some 14% of deputies thought that lack of resources was the reason for not having at least a legislative normative basis for e-voting in Slovenia, which is, according to the findings of Remmert [Re04] and Van Den Besselaar et al. [VODF03] inexcusable, since e-voting could, over time, actually reduce costs (see section 2.1); some respondents saw the reason in the problems of ensuring the 'one voter – one vote' rule, which, according to Estonia, should not be a problem at all, since Estonia used multiple voting to reduce other people's influence on a voter's decision (see chapter 2.1)

It is evident that Slovenia cannot expect the implementation of e-voting in the near future. Our initial hypothesis was confirmed – the current ruling powers were not in favour of e-voting. Right-aligned deputies are much more sceptical about the implementation of e-voting than the left-aligned, which is something to be worried about, since the current ruling collation largely comprises right-aligned deputies.

References

[html1] Rivest, L. R.: Electronic Voting. Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, http://theory.lcs.mit.edu/%7Erivest/Rivest-ElectronicVoting.pdf.

[AP04] Arh, M., Peulič, D.: Profil volivcev posamezne stranke. Gfk Orange No 35, Gfk Gral-Iteo, October 2004, http://www.gfk.si/lnovice.php?NID=1139#.

[Ce05] Cerar, G.: Prezrti estonski zgledi. Mladina (44), October 2005, http://www.mladina.si/tednik/200544/clanek/uvo-manipulator--gregor_cerar/.

[De05] Dečman, M.: Responsiveness of E-Government and the Case of Slovenia. Proceedings of the 5th European Conference on e-Government, ECEG 2005 (Remenyi, D., ed.), University of Antwerp, Belgium 16-17 June 2005. Academic Conferences Limited, UK, 2005.

[GLZ04] Grad, F., Lukšič, A., Zagorc, S.: Ustavno-pravni in politološki vidiki uvajanja e-volitev v RS, Študija izvedljivosti, 2004 http://mid.gov.si/mid/mid.nsf/V/K2633A9BFD03509F2C1256E52005D938F/$file/Evolitve_ustavnopravni_in_politoloski_vidiki.pdf.

[ID03] IDABC. E-voting fails to raise electoral participation in the UK, says independent report, E-government news, 26 June, 2003, http://europa.eu.int/idabc/en/document/1431/358.

[IT04] I. T.: Ali bi bili pripravljeni voliti prek interneta? Delo, Informacijska tehnologija: 08.10.2004. In: Research of Internet in Slovenia, 29.10.2004, http://www.ris.org/main/novice/readnews.php?sid=137.

[Ko04] Kodelja, M.: E-paranoja države. January 2004, http://www.mojmikro.si/articles/60_61_e-volitve.pdf.

[MIS03] Ministry of Information Society: Zasnova študije izvedljivosti elektronskih volitev, Ljubljana, December 2003, http://mid.gov.si/mid/mid.nsf/V/KBF59760A55676EA3C1256E52005DAC22/$file/Evolitve_zasnova_studije_izvedljivosti.pdf.

[NEC04] The National Election Committee: General Description of the E-Voting System. Talinn, 2004, http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf.

[No02] Norris, P.: E-Voting as the Magic Ballot? The impact of Internet voting on turnout in European Parliamentary elections, Paper for the Workshop on 'E-voting and the European Parliamentary Elections' Robert Schuman Centre for Advanced Studies, Villa La Fonte, EUI 10-11th May 2002. http://ksghome.harvard.edu/~pnorris/ACROBAT/Magic%20Ballot.pdf

[Re04] Remmert, M.: Towards European Standards on Electronic Voting. In: Prosser A., Krimmer R. (Eds.): Electronic Voting in Europe − Technology, Law, Politics and Society, Austria, 2004, p. 13-16, http://static.twoday.net/evoting/files/E-Voting-in-Europe-Proceedings.pdf.

[So05] Site officiel de l'Etat de Geneve: Different views of evoting – The Geneva Internet Voting System, October 2005, http://www.geneve.ch/evoting/english/presentation_projet.asp#impact.

[SO06] Statistical Office of the Republic of Slovenia. Usage of information-communication technologies (ICT) in households and by individuals. Rapid Reports No 6/2006 – Information Society. Ljubljana, January 2006, http://www.stat.si/doc/statinf/29-SI-100-0601.pdf.

[Tu04] Turk, M.: Študija izvedljivosti e-volitev s predlogi implementacije, Ministry of Information Society, Ljubljana, February 2004, http://mid.gov.si/mid/mid.nsf/V/K7F5A0C562D52B67BC1256E53003C431B/$file/Evolitve_studija_izvedljivosti_mid.pdf.

[VODF03] Van Den Besselaar, P., Oostveen, A. M., De Cindio, F., Ferrazzi, D.: Experiments with e-voting technology, experiences and lessons. In: Cunningham, P. et al. (Eds.): Building the Knowledge Economy: Issues, Applications, Case Studies. IOS Press, 2003, http://www.social-informatics.net/Bologna2003.pdf.

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER - Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods - Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahnič (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 - Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement - Erfahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometric and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 - Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-86 Krimmer, R. (Ed.): Electronic Voting 2006

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14
53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de

Robert Krimmer, Rüdiger Grimm (Eds.)

Electronic Voting 2008 (EVOTE08)

3rd International Conference
Co-organized by
Council of Europe, Gesellschaft für Informatik
and E-Voting.CC

August 6th-9th, 2008
in Castle Hofen, Bregenz, Austria

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-131

ISBN 978-3-88579-225-3
ISSN 1617-5468

Volume Editors
Mag. Robert Krimmer
Competence Center for Electronic Voting and Participation
E-Voting.CC gGmbH
Pyrkergasse 33/1/2, A-1190 Vienna, Austria
Email: r.krimmer@e-voting.cc
Prof. Dr. Rüdiger Grimm
Universität Koblenz-Landau
Institut für Wirtschafts- und Verwaltungsinformatik
Universitätsstraße 1, D-56016 Koblenz, Germany.
Email: grimm@uni-koblenz.de

printed by Köllen Druck+Verlag GmbH, Bonn
Gedruckt mit Unterstützung des Bundesministeriums für Wissenschaft und Forschung in Wien.

Preface

For the third time Castle Hofen is the meeting place to discuss the current state of the art in electronic voting around the world for academia, administration and vendors in the field. All of these benefit from the high level of interdisciplinarity and interest on all sides.

The past two years have been like a rollercoaster for electronic voting – on one hand there are success stories like legally binding internet elections – on the other hand major set backs as the decision to go back to paper and pencil for elections after years of e-voting experiences.

These experiences show the need for exchange of information and knowledge which has always been an aim of this conference. In the past six years, attendants from over 30 countries have used this opportunity which makes the conference a fixed point in the schedule of e-voting experts from all over the world.

On our call for papers we received over 30 submissions of which we had to select the 17 best for presentation. This was done in a double-blind-review process, that wouldn't have been possible without the tremendous effort, which the programme committee members and the additional reviewers put in the process.

Special thanks go to the Council of Europe and the working group ECOM – E-Commerce, E-Government and Security of the Gesellschaft for Informatik for their support in organizing this conference.

Further thanks go again to the Gesellschaft for Informatik and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Ministries for Science and Research (BMWF), for Interior (BMI), the Ministery for European and International Affairs (BMeiA) and the Regional Government of Vorarlberg for their continued support.

Without the help of the programme committee, who were always available with their advice, the conference would not have reached the status it has today.

Finally we would like to thank Terry Davis, general secretary of the Council of Europe and Jürgen Weiss, vice chairman of the Austrian Federal Council that the conference can take place under their auspices.

Vienna, Koblenz, August 2008 Robert Krimmer, Rüdiger Grimm

Co-Organizers

E-Voting.CC Competence Center for Electronic Voting and Participation

Council of Europe

Gesellschaft für Informatik
Working Group for E-Commerce, E-Government and Security

Introductory Words

New communication technologies have a tremendous potential for empowering people. Millions of people engage in all sorts of electronic transactions. They download information online or through their mobile telephones.

Democracy is part of this development. There have been many experiments with voting through the Internet, voting on computers in polling stations, and even voting by digital TV or mobile phone.

While experimenting with these forms of voting, some important new issues, in comparison to traditional voting, come up. How does one observe voting through a computer? Or counting such votes? How does one guarantee a transparent election when people vote on a machine? Security and legal aspects also play an important role in the voting process.

In 2004, the Committee of Ministers adopted a Recommendation on E-Voting, which is the first and so far the only existing international text setting standard for electronic voting. The application of this recommendation is reviewed every two years at a Council of Europe meeting to keep up with the rapid developments in the use of information technology. This conference is a part of the process; it is one of the few conferences that brings together governments and international organisations, academia and the business sector, in order to discuss their experiences with e-voting.

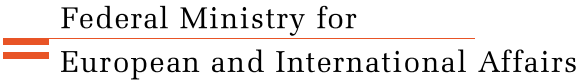
Right Hon Terry Davis

Secretary General of the Council of Europe

Supporters


BMWFa
Bundesministerium für Wissenschaft und Forschung


BM.I
BUNDESMINISTERIUM FÜR INNERES


Federal Ministry for
European and International Affairs


Vorarlberg
unser Land

Introductory Words: Today more Democracy means E-Voting

E-Voting gives us an important opportunity to obtain more democracy and more civil participation. Therefore, we have to welcome every consideration and all possible instruments of electronic voting in Austrian—for elections, for binding or non-binding consultative referendums as well as in petitions. We have to see e-voting as a chance to offer more services for citizens, to promote a plus in the voter turnout and also in the use of direct democracy.

As our behaviour and our possibilities in many aspects of our lives are changing, our election system should also evolve to meet the needs of contemporary society. For people becoming more and more mobile, it is also necessary for politics to keep up with recent trends and to give democracy new chances. All together, we could launch a sensible realisation. So it must be beyond doubt that the secrecy of ballot obtains first priority.

Nowadays, although everyone surely deals with his or her money very carefully, we trust the Internet enough to carry out bankingtransactions and shopping excursions online. ,In postal voting we trust in the post, and in E-Voting there are even more elaborate solutions that make the process secure and anonymous.

I take questions, doubts or even fears very seriously. Democracy contains dialogue and this has to be led. At the same time, however, I find it incomprehensible that in times of decreasing voter turnouts this additional possibility for citizens to make use of their right to vote, which means a possibility for more democracy, seems not to be recognised as such. In the view of growing disenchantment with politics, no one can shut their eyes.

E-Voting may – especially for young people – be an incentive to vote effectively. I think that particularly the young generation will make use of this new technology rather than of the previous instruments. Several countries have shown that the system is accepted. My aim in Austria is to show how E-Voting works. Therefore, I would like to offer this additional way of voting for the first time at the elections for the Austrian National Union of Students in 2009. The legal base is already established, the technical preparations well advanced. Now it is necessary to motivate students to smooth out potential concerns commonly and to make use of this new way of voting!

I wish the participants of the conference many new scientific insights and a pleasant day.

Dr. Johannes Hahn

Austrian Federal Minister for Science and Research

Partner

All presentations are available in Audio & Video including slides at http://www.e-voting.cc/2008 with the help of

Introductory Words

The current working program of the Austrian Federal Government includes the introduction of postal voting as well as the examination of the use of electronic voting. The first part of this program, postal voting, was implemented in 2007 and has already been proven in practice during the regional elections in Lower Austria in March of this year. With regard to E-Voting, the different premises are currently being evaluated by the Ministry for the Interior and according to the head of the Austrian electoral management board, implementing E-Voting in Austria could be implemented on relatively short notice.

The federal minister for science and research has announced the use of E-Voting as an additional voting channel for the Austrian student-union's elections in 2009. This is possible because the legal basis was installed beforehand. As students have profound knowledge in the daily use of the Internet, they are a perfect target group for this pilot-test. The Austrian Federal Economic Chamber could also be a possible e-voting election as the legal basis exists as well.

In all these cases E-Voting does not mean the use of voting machines to facilitate the counting of the votes, it rather offers a further voting channel via the Internet, along with the familiar voting ballot at the voting station and postal voting. Although E-Voting is mainly a channel to vote at elections, it will also play an important role in referendums, plebiscites as well as petitions for referendums. The use of all these instruments will facilitate the citizen's participation in the political process. This may specially be the case where elections have non-binding character or with regard to elections with specific target groups. Experience with periodic surveys among employees of large enterprises has shown that anonymity can be secured without large efforts and e-voting also leads to high participation rates in these cases.

Bearing in mind the long time it took to introduce postal voting in Austria and the immense doubts it has raised with respect to secrecy of the vote and prevention of misuse, we can anticipate how much work still needs to be done before e-voting can finally be introduced. According to the latest polls, around sixty percent of the Austrian population are still sceptical of E-Voting. One part of these doubts is not nourished by knowledge of facts but by mere feeling. To create a field of trust around E-Voting we need to experience pilot tests and get used to the thought that electronic electronics are a part of the electoral process. Initially it is a challenge for scientists to which the "Competence Centre for Electronic Voting and Participation" commendably contributes by organizing this conference in Schloss Hofen every second year. Thereby international exchange of experience plays an important role – also experiences from abroad can convince. I therefore wish the EVOTE08 Conference and its participants in my home region Vorarlberg a comfortable location for fruitful scientific work.

Jürgen Weiss, Vice President of the Austrian Federal Council

Programme Committee

- Mike Alvarez, USA
- Frank Bannister, Ireland
- Jordi Barrat, Spain
- Josh Benaloh, USA
- Nadja Braun, Switzerland
- Thomas Buchsbaum, Austria
- Chantal Enguehard, France
- Simon French, UK
- Ruediger Grimm, Germany
- Thad Hall, USA
- Catsumi Imamura, Brasilia
- Norbert Kersting, South Africa
- Shin Dong Kim, Korea
- Laurence Monnoyer-Smith, France
- Hannu Nurmi, Finland
- Wolfgang Polasek, Austria
- Michael Remmert, France
- Josep Reniu, Spain
- David Rios, Spain
- Fabrizio Ruggeri, Italy
- Kazue Sako, Japan
- Berry Schoenmakers, Netherlands
- Robert Stein, Austria
- Dan Tokaji, USA
- Alexander Trechsel, Switzerland
- Melanie Volkamer, Germany
- Poorvi Vora, USA
- Dan Wallach, USA
- Gregor Wenda, Austria

Additional Reviewers

- Navarro Ángel Sánchez, Spain
- Joakim Astrom, Sweden
- Carol Boughton, Australia
- Danilo Bruschi, Italy
- Osvaldo Catsumi Imamura, Brasil
- David Canning, UK
- Letizia Caporusso, Italy
- Gerard Cervello, Spain
- Michel Chevallier, Switzerland
- Jeremy Clark, Canada
- Ishbel Duncan, UK
- Joao Falcao e Cunha, Portugal
- Joao Faria, Portugal
- Rosa M. Fernandez, Spain
- Stefanos Grizalis, Greece
- Tina Jukic, Slovenia
- Sokratis Katsikas, Greece
- Karl-Heinz Ladeur, Germany
- Costas Lambrinoudakis, Greece
- Ylle Madise, Estonia
- Tarvi Martens, Estonia
- Marc Mausch, Germany
- Rebecca Mercuri, USA
- Lilian Mitrou, Greece
- Peter G. Neumann, USA
- Goran Obradovic, Canada
- Anne-Marie Oostveen, Netherlands
- Ana Paiva, Portugal
- Emilia Perez Belleboni, Spain
- Joan Josep Piles, Spain
- Miguel Pimenta Monteira, Portugal
- Judith Rossebo, Norway
- Emilia Rosti, Italy
- Jose Ruiz, Spain
- Christian Rupp, Austria
- Peter Ryan, UK
- Jose Luis Salazar, Spain
- Gorm Salomonsen, Denmark
- Guido Schryen, Germany
- Frederic Solop, USA
- Aleksandra Sowa, Germany
- Tim Storer, UK
- Kare Vollan, Norway
- Michel Warynski, Switzerland
- Alexandros Xenakis, UK

Content

Overview

Robert Krimmer[1], Rüdiger Grimm[2]

[1] E-Voting.CC
Competence Center for Electronic Voting and Participation
Pyrkergasse 33/1/2, A-1190 Vienna, Austria
r.krimmer@e-voting.cc

[2] Universität Koblenz-Landau
Institute for Information Systems Research
Universitätsstraße 1, D-56016 Koblenz, Germany
grimm@uni-koblenz.de

Democracy and elections have more than 2,500 years of tradition. Technology has always influenced and shaped the ways elections were held. Today elections are the core element of democracy as a society's way to make decisions. Elections are the way to express how societies use technology and as new technologies emerged and evolved, elections changed accordingly. While there have been democratic structures in societies like India or Babylon, the birthplace of democracy is attributed to old Athens in 507 BC. From thereon similar structures of direct democracy, bound by face-to-face societies, also developed in several places around the world like in ancient Rome, with the Vikings or in the Cantons of Switzerland. The next level of democracy developed with the creation of nation-states in the late 18th century with the need for representatives. This form of indirect democracy spread from the United States and France around the globe to today's predominant role of democracy as a rule of government and was mainly limited by the nation's borders.

One can see this development as three comings of democracy:

1. The Face-to-Face Society
2. The Territorial Society
3. The Global Society.

With the latest emergence of technology we face a new challenge to spread the influence of one country around the globe to allow out-of-country voting and enable disenfranchised voters. This leads to multiple effects on the electoral process including e-campaigning, electronic supported candidate nominations, central voter registers, electronic elegibility checks in polling stations, to casting votes electronicly and support for result or mandate calculation. This development is not uniform in all countries but can be observed everywhere to some extent.

It is the task of this conference series to enable the discourse amongst researchers, administrators and vendors so that understanding, cooperation and future research can emerge. As such this year's conference concentrates around eight core topics.

The first session deals with the different experiences made with E-Voting in the Netherlands and in Estonia. During the last two years the Dutch E-Voting system has been successfully challenged by activist groups which have led to a stop of electronic voting. The paper of *Leontine Loeber* gives an analysis of the situation. *Epp Maaten* and *Thad Hall* then will give an overview of the Estonian E-Voting experiences. Technically and politically the Estonian system has been used twice in practice. The authors suggest improvements which could be made with regard to enhancing the transparency of the voting system.

In the second session the coherence between electronic voting devices and voting outcome is discussed by *Gabriel Katz, Michael Alvarez, Ernesto Calvo, Marcelo Escolar* and *Julia Pomares.* Their study estimates the effect of different E-Voting technologies on the likelihood that citizens cast their vote for different parties for the National Congress and the Legislature of Buenos Aires and shows considerable effect. *Alicia Kolar Prevost* then presents her findings that programs designed to make voting easier have not succeeded in boosting turnout, and have even had the unintended consequence of exacerbating the demographic biases that already exist in the electorate. She will give an outlook to the implication this could have on future voting reforms.

Session three will deal with the paper by *Komminist Weldemariam* and *Adolfo Villafiorita.* They present a methodology for procedural security analysis in order to analyze and try to make elections more secure. Their approach is based on modelling the electoral procedures in the form of business process models. *Victor Morales-Rocha, Jordi Puiggalí* and *Miguel Soriano* will show the importance of an accurate voter register and will present a scheme to improve this vital aspect. Further on recommendations on long-term retention in E-Voting will be given, applying the results of *Rotraud Gitter, Lucie Langer, Susanne Okunick* and *Zoi Opitz-Talidou* to a state-of-the-art E-Voting scheme. They will also review technical measures to meet the security requirements of long-term retention in E-Voting.

The fourth session deals with comparing the E-Voting experiences in different countries. First *Robert Krimmer* and *Ronald Schuster* present a methodology on how to measure the context of E-Voting in 31 countries. Then *E. John Sebes* and *Gregory A. Miller's* paper compares and analyses the E-Voting experiences in the US, which have been disenchanting, with the experiences in Europe where E-Voting is more and more adopted.

The topic of the fifth session are new and improved protocols. *David Lundin* presents the Prêt à Voter voting system. It is characterized through very high security properties. His working group aims to make the system truly applicable for elections with many races and various candidates by allowing the vote to be formed using a voting machine and by printing a minimalistic receipt. A concept is also presented to secure electronic voting systems. The Farnel voting scheme will be discussed by *Roberto Araújo* and *Peter Y. A. Ryan.* This concept will be improved through trustworthy talliers. Further they will present a novel way to initialize the Farnel box and a new scheme based on combining Farnel with Prêt-à-Voter style encoding of receipts.

Session six's discussion is concentrated around certification of E-Voting systems. *Melanie Volkamer* and *Rüdiger Grimm* present an approach of a formal trust model for remote electronic voting which is needed for an in depth analysis of E-Voting systems. *Jordi Barrit i Esteve* then discusses the different approaches on how to certify E-Voting machines in Europe as well as publication requirements.

Technological issues around code voting are dealt with in session seven, where *Jörg Helbach*, *Jörg Schwenk*, and *Sven Schäge* propose the application of group signatures for it. *Rolf Oppliger*, *Jörg Schwenk* and *Christoph Löhr* use a different approach to code voting with CAPTCHA.

The last session then gives room to political issues. Here *José Rodrigues Filho* goes about E-Voting in Brasil where he discusses the role of institutions. The voting process in participatory budgeting builds the final part of theese procedings where *Cristiano Maciel* and *Gleison Pereira de Souza* present a case study.

As can be seen from the contributions in this conference the discussion on E-Voting has not been decided yet. Moreover the research needs are highly interdisciplinary and discourse amongst the disciplines has to be an aim of any future research. As such we hope that Castle Hofen will give a good place for this in the future.

Session 1: E-Voting Experiences

E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years

Leontine Loeber

Dutch Electoral Council
Herengracht 21
2500 EA Den Haag
The Netherlands
Leontine_Loeber@xs4all.nl

Abstract: This document is a case study of a country in which e-voting used to be the general norm: The Netherlands. It gives a detailed description of the events in the last two years surrounding e-voting in the Netherlands. During this time, the security and reliability of the voting machines that were used were questioned successfully by an action group. This led to court cases, the withdrawal of the certification of these machines and eventually to a complete stop of their use. In the current situation, The Netherlands reverted back to paper ballot voting at least until a whole new system is designed, approved of by Parliament, built and implemented. In this document the author tries to explain why this happened at this particular time. The paper concludes with some ideas on what other countries that are considering the introduction of e-voting might learn from the Dutch experience.

1 Introduction

The last two years have been a rollercoaster for those involved with e-voting in the Netherlands. During the municipal elections of March 2006, nearly 99% of the voters cast their vote with the use of a voting machine. Both in the 2004 European Parliament elections and the national elections of November 2006, the voters living abroad could use the internet as a channel for voting. During the European Parliament elections of June 2009, both groups of voters will have to use the traditional methods of paper ballot and postal voting. It is still uncertain if e-voting will return shortly after those elections. Where the introduction of the use of voting machines in legislation in 1965 happened without any discussion and parliament was, as recently as 2005, asking for the introduction of internet voting for all voters, they now have an unprecedented interest in every little step that the Cabinet takes in regards to this subject.

What happened in the Netherlands to cause this complete turn away from e-voting and what are the prospects for the future? This paper will try to give more insight in the events that caused this landslide.

2 Voting machines

2.1 Legal Requirements for the Use of Voting Machines

The Dutch legislation on elections was set up in such a way that the election process that is used when voting with a paper ballot was also applicable to voting with voting machines. Only in the situations where voting with a machine significantly differs from voting with ballot papers, exceptions were made in lower legislation. Because the two processes existed alongside each other, there has never been, until now, a fundamental discussion concerning the question as to whether the introduction of e-voting should lead to a reconsideration of the way the fundamental principles of free, fair and secret elections are guaranteed.

The Dutch Elections Act was, as stated above, based on the principle of voting by paper ballot. It only contains three provisions regarding e-voting[1]. These provisions state that electronic voting is possible and give some general demands for electronic means that are used in the voting process. The most important requirement in the act is a certifying procedure. The act also states that the means must guarantee the secrecy of the vote. All other regulations for voting machines were found in lower legislation in chapter J of the Decree of 19 October 1989, establishing new regulations for implementing the Elections Act and the ministerial Regulation for the approval on voting machines 1997.

To obtain an approval, a supplier had to submit a prototype of a machine to an independent certification agency that tested the machine against the requirements stated in the ministerial regulation. The test results were not made public. Based on the test report of the agency, the supplier could apply to the Minister of the Interior for an approval of the prototype. Once the prototype was approved, the supplier gave the agency ten machines of which the agency tested one against the prototype. If the tested machine was built according to the approved prototype, the agency would conclude that the machine could be approved. Again, for the final approval, the supplier had to apply to the Minister. The regulation had an appendix which contained the demands that a machine had to meet before it could be approved. These demands had not been updated since the regulation came into force in 1997. The regulation also contained a number of grounds based on which the Minister could decide to withdraw a given approval.

[1] The articles J 32 to J 34 in the Dutch Elections Act.

2.2 History of Voting Machines

The use of voting machines in the polling station has known a long tradition in the Netherlands. Already in the 1950's there was interest for the electronic voting machines used in the United States. In 1966 the first machines of this type, made by Automatic Voting Machine Corporation (AVM), were introduced in the Netherlands. In 1965 the Electoral Act was modified in the sense that the possibility of elections with the use of electronic means was opened. It was left up to the municipalities, who are under Dutch law responsible for organising elections, whether they wanted to use machines or not. The legal provisions called for an approval of voting machines by the Minister of the Interior after which municipalities either bought or rented the machines from the suppliers. This led to a situation where, in 2005, there were two suppliers who divided the market: Nedap and Sdu. Nedap built voting machines with panels that were big enough to contain all the candidates for an election[2]. They were one of the first companies to build voting machines for the Netherlands and they supplied machines to approximately 90% of the municipalities. They are also active in other countries.

The Sdu machines are smaller and have a touch screen instead of buttons. The voting on these machines is done in two steps, whereby a voter first chooses a party and then, from the list of that party, a candidate. Sdu does not sell the machines to the municipalities, but rents them per election. Both types of machines are stand alone machines, although the Sdu machine does have a GPRS connection. This connection can only be used once the election is closed to send the results to the municipality.

2.3 Fraud during the Municipal Elections of 2006

In one municipality, there was a suspicion of fraud during the 2006 elections. A certain candidate obtained 181 preferential votes in one polling station. In all the other polling stations together he only obtained eleven votes. The fact that he was a polling worker and the person controlling the voting machine in the polling station where he got the large number of votes, led to an investigation. However, because the Nedap machine that was used does not have a paper trail, a manual recount of the votes was not possible. The District Attorney therefore asked all the voters to come in for a shadow election. The voters were asked to secretly cast their vote again. During this election the candidate only got a very small number of votes. Also, a number of voters testified that they felt that the suspect had told them too early that they had cast their vote. This gave the District Attorney enough reason to indict. The court in lower instance acquitted the suspect due to lack of evidence. However, when the District Attorney appealed, the appellate court did decide to convict. They found that the testimonies, combined with the results of the shadow election, gave enough cause to convict the suspect of election fraud. This case made people wonder if fraud was possible while using voting machines and if so if fraud had happened before. Was this person the first, or was he just caught because in his case it was so obvious?

[2] The Dutch system is based on a preferential vote for a candidate. In a general election, approximately 600 candidates compete.

2.4 Campaign by NGO we don't trust voting computers

In 2006 an action group by the name of we don't trust voting computers was founded[3]. This happened after the municipal elections of March 2006 during which the municipality of Amsterdam used voting machines for the first time. Most of the founders of the action group live in Amsterdam and were confronted with these machines. The leader of the group is Rop Gonggrijp, a well-known hacker and founder of the internet company xs4all. They started their campaign in the spring of 2006 with a series of requests based on the Freedom of information act. Through these requests they wanted to obtain as much information as possible concerning the voting machines and the decision making process surrounding the approvals. They also approached municipalities in an attempt to buy voting machines. This was successful; they managed to get a couple of Nedap machines. While they were doing this, the Cabinet fell and it became clear that there would be general elections in November.

The action group managed to decipher the operating system for the Nedap machine and wrote an overwrite program that would make it possible to commit fraud with the machines. This program would transfer a certain number of votes casts from one candidate to another. Because the machine did not have a paper trail, this fraud could go undetected if applied on a small scale. While examining the machine, the action group also detected that the radiation transmitted by the screen on the machine can be read from a distance[4]. This makes it possible to break the voter secrecy since in the Netherlands the name of a voter is read out loud in the polling station. The action group presented their finding during a press conference on October 4th [Gr06]. Although the fraud possibility is probably the biggest problem since it changes the outcome of the election, most attention went to the question of voter secrecy. This is caused by the fact that secret elections are not only guaranteed by the Dutch constitution, but also a requirement in the first protocol of the European Convention on Human Rights. The Dutch government is therefore obliged to do anything in their power to guarantee a secret election.

[3] The Ngo has a website, www.wijvertrouwenstemcomputersniet.nl, which also contains information in English.

[4] In computer science, this is known as the Tempest problem. The problem was detected in normal computers as early as the 1980's.

The Cabinet decided after the press conference to have the Secret Service test all types of machines in use for this Tempest problem. It turned out that the most common used Nedap machines did not radiate beyond 5 metres. The Sdu machines however could be 'read' from a distance of over 30 metres, due to their larger screen. This was such an uncontrollable situation that the Cabinet did not see any other option than to withdraw the approval of these machines, even though it was only three weeks before the election. The election did take place, with a crisis team supporting the 32 municipalities whose Sdu machines could not be used. Ten of them were able to use Nedap machines and in 22 municipalities, including Amsterdam, the voting was once again done with paper ballot and pencil. During the elections, which were observed by the Organisation for Security and Cooperation in Europe, there were no major problems with the voting machines [OD07]. The extra security measures that were taken seemed to function well, and although five machines were taken out of service because they might have been tampered with, tests revealed that they were all functioning normal.

After the elections preparations had to be made for the Provincial elections of March 2007. Sdu went to court to fight the withdrawal of their approval and managed to get a court order for a new test by the Secret Service. Although they got a number of attempts, they did not manage to deliver a machine with a radiation range under 5 metres. It was then decided not to renew their approval. For the elections, the same security measures as during the general elections were in place and everything went well.

2.5 Advisory Committees

The events surrounding the general elections led to an increased attention from Parliament. They asked the Minister to set up two independent advisory committees. The first looked into the past, especially to the decision making process concerning the use of voting machines. This committee published a report in April 2007 that stated mistakes had been made in the past. One of the major issues they detected was that the ministry did not have enough technical knowledge, which led to a situation where the suppliers not only controlled the market, but were also influential in the decision making process. Also, the responsibility for the elections and the electoral legislation had in the past shifted several times between different parts of the ministry. This caused a shattered knowledge of the system and its origins. Just before the elections of November 2006, it was not clear which division was responsible for what, which led to an inability to respond quickly to the problems that arose due to the criticism on e-voting. Furthermore, the committee concluded that the embedding of the voting machines within the legal framework was very weak. The lack of technical knowledge had caused a certification process in which the security of the machine was not tested properly. Therefore, they recommended an update of the regulation concerning the certification of the voting machines [He07].

The second committee was asked to give recommendations regarding the electoral process in general and on new ways of e-voting in particular. They published their report 'Voting with Confidence' on September 27th of 2007. One of the recommendations was that the Minister of the Interior should get more responsibilities in the electoral process. This would mean that the current legal position of the municipalities in the process would be changed. Another recommendation concerned a new way of using technology in the voting process. In light of the problems that arose because of the lack of a paper trail with the old machines, they recommended a new system. This system would consist of a voter printer and a vote counter machine. The printer should basically function like a pencil; the voter selects a party and then a candidate, after which the printer would print this selection. The printer does not store the votes. The voter takes the print and puts it in a ballot box. At the end of the day, the votes are counted with the vote counter, which is a scanner [Ka07]. The main advantage of this system over the traditional paper ballot voting is that it prevents voters from casting unintentional invalid votes. It also makes it possible to adapt the system for blind people, for example through the adding of a voice recorder. Last, it speeds up the counting process. Compared to the current system of voting machine, the main advantage lies in the paper trail and the fact that the voter can check whether the printer printed the vote correctly before casting it. Therefore, the proposed system does not require a high level of trust in technology by the voter.

2.6 Aftermath

During the press conference in which the 'Voting with Confidence' report was presented, the State Secretary for the Interior announced that the 'Regulation for approval of voting machines 1997' would be withdrawn. The action group had already filed a court case against the approval of the Nedap machines given in March 2007. As a result of this procedure, on October 1st 2007, the District Court of Amsterdam decertified all Nedap voting machines that were in use in The Netherlands. Since the approval of the Sdu machines was already withdrawn, there were no more certified machines at that time. On October 21st 2007 the 'Regulation for approval of voting machines 1997' was actually withdrawn. Also, the Decree of 19 October 1989 was amended, taking out the provisions that gave the Minister the competence for making new regulations for the approval of voting machines. Therefore, it was also no longer possible to certify new machines. This means that until new e-voting mechanisms are developed and the rules concerning their use are entered into legislation, the current legislation only allows for voting by paper ballot. However, Nedap did file an appeal against the decertification order by the District Court. They also lodged a complaint with the Ministry of the Interior against the withdrawal of the regulation. The State Secretary has recently decided to uphold the withdrawal decision. It is expected that Nedap will also file an appeal in this case. Both cases are therefore still running, so the situation might change once again in the near future. Since it is uncertain when the ruling in these cases will come and what the outcome will be, municipalities, the ministry and the Electoral Council have started preparations to hold the first nation wide election with paper ballots in over 40 years.

3 Internet and Telephone Voting

3.1 Experiments

In 1999 a project was started to investigate possibilities for remote e-voting. This project was in first instance mainly meant for voters from abroad. The intention of the Minister at that time was however to also in time expand the possibility of remote e-voting to voters within the Netherlands. The voters from abroad were seen as an ideal test group for this type of e-voting. Since 1985 almost all Dutch citizens living abroad have been eligible to participate in elections. The main requirement for them is that, in contrast to voters living within the Netherlands, they have to register separately to become a voter. Before 2004 they could choose to vote by mail, by proxy, or in person in a polling station within the Netherlands. Approximately 25000 voters register per election to participate. The procedure for voting by mail was seen as problematic and time-consuming and not all the votes were received in time to count in the elections. Therefore, an experiment was held during the European Parliament elections in 2004 whereby voters from abroad could choose to vote via the internet or the telephone. During the registration process they had to apply for this. The experiment was held under special legislation, the Online Voting Experiment Act. The Internet voting was a success; the telephone experiment was only used by a very small number of voters. Because of these results, the government decided to abandon the telephone experiment, but to carry on with the internet voting. During the national elections in 2006 a new experiment was held with the internet voting. Again, this was a great success; out of the 34.305 registered voters from abroad 21.593 voters (63%) chose to vote via Internet in the registration period. During the elections, 19.815 voters (92%) did eventually cast their vote through the Internet. These voters were asked to fill in an online questionnaire on internet voting. 11.003 voters (65%) responded to the questionnaire. Out of these voters, 99% preferred internet voting over voting via mail. 94% wanted the government to implement internet voting permanently[5].

3.2 Future

These figures and the positive experiences of the governments working with internet voting, led to the plan to implement internet voting for voters from abroad into the regular Election Act, since there was no reason to keep experimenting.

[5] See also www.minbzk.nl/bzk2006uk/subjects/constitution-and/internet-elections

However, the controversy surrounding the voting machines also rubbed off on the discussion surrounding internet voting. If a certifying procedure was deemed necessary for the machines, then why not for the internet service that was used during the election process? This question was asked by Parliament in a discussion with the State Secretary for the Interior in November 2007. The Parliament adopted a motion stating that a certifying procedure should be installed for internet voting. In January 2008 the State Secretary announced that the instalment of such a procedure would cost a lot of time and money and that it was therefore not possible to allow voters from abroad to vote via the internet in the European Parliament elections of 2009. Just before this announcement, the action group filed several Freedom of Information requests concerning internet voting. Now that the voting machines are out of the way, at least for the moment, it looks like the future of internet voting is going to be the next topic of debate in the discussion surrounding Dutch Elections. It is therefore still very uncertain if internet voting will in the future become a permanent option. The demand for nation-wide internet elections that Parliament still made in 2005 has not returned on the agenda and probably will not for a long time.

4 And now?

On the 30th of January 2008 the Parliament debated the proposed new system with the Minister. Several of the parliamentary fractions called for a very thorough approach and made it clear that they would rather vote with paper ballots a bit longer than to rush into new ways of electronic voting. The State Secretary decided to set up a technical advisory committee to examine the feasibility of the new system and to set up guidelines for the technical testing of the vote printer en counter. The results and recommendations of this committee are not known at this moment. They will report to the Minister shortly, as she had promised Parliament that Cabinet will decide on the future of this system before May 1st. Since then, she has announced that this decision will be delayed until probably half May. Already it has been made clear that the 2009 elections for the European Parliament will be held with paper ballot voting. After all, even if the Cabinet and Parliament decide to implement the new system, it will not be possible to develop and test it in time for these elections. This means that currently the Dutch municipalities are in the process of preparing elections in the old fashioned way. For a large group of voters this will mean that they will have to vote with paper for the first time in their lives, even though they have been voting for 30 years. A lot of effort will have to go towards explaining to these voters how this works. What will happen after the European Parliament elections is still a big mystery, even for those involved in the decision making process at this time. The biggest question is whether it will be possible to design a new system for electronic voting that can withstand the fast changes in computer science and the pressure of anti e-voting group and at the same time be voter friendly, easy to use and not too costly.

5 Conclusions

The mere fact that the introduction of voting machines in the Netherlands did not lead to discussion and seemed to go rather smoothly did not ensure that this topic would not be controversial later on. On the contrary, because the introduction went so easy, maybe the political attention for the subject was not great enough, causing neglect and a lack of knowledge with both the Ministry and the Parliament. New developments in computer science and security issues were not linked to voting machines even though there was enough reason to do so. A note hereby however is that also computer scientists have only recently started to consider the subjects of trust, transparency and verifiability in relation to the use of computers in elections. The consequence was that only when the actions of an action group led to a major crisis on the subject, was it acknowledged that there might be a problem.

What can we learn from this? First of all, an important lesson is that the introduction of e-voting should be accompanied by intensive testing. If possible, in this procedure both supporters and critics of e-voting should be involved. Another valuable lesson is that once e-voting is introduced government can not step back and let the market and suppliers take over. Close supervision is necessary to ensure the guarantees of fair, free and secret elections. It is also necessary to reconsider choices that have been made in the past to embed these basic principles in the electoral process. It is not correct to think that voting with a computer is almost the same as voting with a pencil and that the same rules can apply. Issues of transparency, voter secrecy and verifiability will have to be guaranteed, no matter which system you use. But the manner in which these fundamental demands are guaranteed in the process will have to differ. This means that when a change to e-voting is being considered, this has to involve a complete review of the voting process and most likely, an adaptation of certain rules and procedures. This prevents problems later on that might lead to the decline of trust in the system.

A last lesson is that once trust in the voting system declines, it is hard to win this back. Without this support, the legitimacy of the chosen legislator will diminish. It is therefore important to realise that the fact that e-voting can work in one country does not automatically mean it is suitable for all countries. A lot depends on the general level of trust in government, but also the level of trust in the corporations that supply the machines use in the electoral process. If government or the corporations are seen as biased towards certain parties or candidates, the use of voting machines will most likely fuel suspicion of fraud within the elections. In the Netherlands, there is a trend of declining trust. This trend is not only visible in the case of e-voting, but also with other technical solutions. In a recent case, government wanted to introduce a chip card as a means for payment in the public transportation system. This card would replace the current paper payment method. A lot of people feared that this could compromise the privacy of the traveller, especially after some experts proved it was possible to hack the card and read its contents. The further introduction of the card has once more become a topic of debate. Even trust in government in general seems to be declining. In the autumn of 2001, 70% of the voters expressed trust in political government. In the spring of 2004, this number had fallen to only 39% [AI05]. It is therefore not quite unexplainable that the controversy surrounding e-voting only started very recently.

Finally, it is important to realise that elections are not like other areas where computers are being used. E-Voting is often compared to electronic banking. There are, however, big differences between the two. First, with banking there is no need for public accountability of the system. It is sufficient if there is an independent auditor. With elections however, every voter should be able to verify that the system works correctly. If this is not possible, trust in elections and thereby trust in the legislator will decline. Another difference is that with electronic banking, a bank can afford a minor system problem once in a while. Mistakes caused by these problems can be corrected. They will also most likely be detected because millions of people can and will check their bank statements. With elections, there is no possibility for corrections. Even if detected, any minor glitch in the system can have a major impact on the question as to who will rule the country for the next four years. A few of these mistakes and the trust is gone, which can have disastrous effects. Therefore, there should be little room for experiments with new technology in elections. This does not have to mean that there is no future for e-voting. It does mean that new systems should not be used in legally binding elections without rigorous scrutiny and certification. And even when the system passes these requirements, it will always be necessary to re-evaluate the system and the certification of it on a regular basis.

References

[AI05] Andeweg, R.B.; Irwin, G.A.: Governance and Politics of the Netherlands. Palgrave MacMillan, New York, 2005; pp. 228-229.

[Gr06] Gonggrijp, R. et. al.: Nedap/Groenendaal ES3B voting computer a security analysis, October 6, 2006, to be found on www.wijvertrouwenstemcomputersniet.nl.

[He07] Hermans, L. et. al.: Voting machines, an orphaned subject", Report by the Advisory Commission regarding the decision making process for voting machines, April 17, 2007, only available in Dutch through the Ministry of the Interior and Kingdom Relations.

[Ka07] Korthals Altes, F. et. al.: Voting with confidence", Report by the Election Process Advisory Commission September 27, 2007, to be found on www.minbzk.nl.

[OD07] OSCE/ODHIR: Final Report on the 22 November 2006 Parliamentary Elections in The Netherlands, March 12, 2007.

Improving the Transparency of Remote E-Voting: The Estonian Experience

Epp Maaten[1], Thad Hall[2]

[1]National Electoral Committee
Lossi pl 1a, 15181 Tallinn, Estonia
epp.maaten@riigikogu.ee

[2]Institute of Public and International Affairs, University of Utah
260 South Central Campus Drive, Room 252
Salt Lake City, UT 84112, USA
thadhall@gmail.com

Abstract: Pilot projects in the area of remote e-voting have been carried out in several countries but the number of those projects in which the Internet-cast votes are legally binding remains small. Estonia, indeed, has been the first country to introduce Internet voting in which legitimate results were obtained at the national level. In local government elections in October 2005 and March 2007 parliamentary elections, Internet balloting was used without controversy. The number of I-voters was three times higher in 2007 compared to 2005.

Elections need to enjoy broad public confidence to be a legitimate, meaningful democratic exercise. Remote e-voting has twice been offered as an additional channel to Estonian voters, and in both cases the system's operation has been considered successful, both technically and politically. Technically, all systems and procedures functioned well and there were no security problems. Politically, the election results were legitimate and there were no proceedings initiated to challenge the Internet voting option.

This paper gives an overview about tools for voters that reduce the negative effects of remote e-voting and improve confidence in the new voting system. A question will be proposed how the observation of remote Internet voting can be put in practice in order to resolve the transparency problems. After two Internet-enabled elections, international observers and researchers have made many recommendations regarding how to improve the transparency of the electoral administration. The paper discusses whether the recommendations focusing on testing, auditing and certification of the voting system are applicable in the light of Estonian experiences.

1 Introduction

Internet voting (I-voting) represents new opportunities for improving the electoral process, but it also presents new challenges. In particular, it is critical that I-voting is introduced in a manner that safeguards the transparency of the elections, which is one of the fundamental principles for democratic elections[6]. I-voting, like other changes in the mechanisms used to capture votes—from paper ballots to voting machines—is a technology that changes the direct means of participation but not the nature of democracy itself. We should, therefore, seek to determine how we can integrate this new technological solution into the old traditions of voting.

The basic question in electoral administration no longer focuses on whether new technology developments are acceptable in electoral processes but rather on what kind of technology is suitable for a specific country, taking into account its political and social culture, level of technological infrastructure, and its electoral system. In the Estonian case, the preconditions were favourable for introducing the most ambitious change in the nature of voting – voting over Internet. It can be clearly said that the Public Key Infrastructure (PKI), the digital signature, and the existing process of authentication have served as absolute prerequisites for the creation of an efficient e-country. Internet voting is just part of the overall concept of e-governance in Estonia [Ma07]. Good communications infrastructure, voters' high e-readiness, the widespread use of the national ID card, which enables securely to authenticate on-line voter, and its relatively small population of 1.3 million complete the list why I-voting has been a success in Estonia.

The argument in this paper is that Estonia's current election system—which includes I-voting as a mechanism for voting—has a high level of legitimacy and transparency on three levels: political/legal legitimacy, voter transparency, and system transparency. At each level, the legitimacy can be measured through the actions of government, the actions of voters, or the actions of the electoral administrators in charge of elections. At each level, participants have been able to engage the system in the most transparent ways possible. The next sections detail the importance of transparency in elections, providing a theoretical framework for appreciating the importance of transparency in elections.

2 Transparency in Elections

Transparency is an internationally recognized principle for elections. The Administration and Cost of Elections (ACE) Project[7] has developed a set of standards for elections, with transparency a critical component. As they note[8]:

[6] See HW08a and HW08b for a summary of the literature on electoral transparency.
[7] The eight entities who are ACE Partner Organizations are: Elections Canada, EISA, Instituto Federal Electoral (Mexico), IFES, International IDEA, United Nations Development Programme (UNDP), the United Nations Department of Economic and Social Affairs (UNDESA), and the United Nations Electoral Assistance Division.
[8] http://aceproject.org/ace-en/topics/ei/ei20 accessed February 22, 2008.

”Transparency makes institutional systems and the actions/decisions they take widely accessible and understood… Electoral administrators and election officers should be held accountable for decisions they make when administering elections; legislators should be held accountable for the content of the laws they pass and the level of funding allocated for elections…[It] builds understanding of the process, the difficulties encountered, and why electoral administrators and election officers make certain decisions. Transparency increases the credibility of the process and the legitimacy of the results. If the electoral process is free and fair, accurate, transparent and monitored, and if laws and regulations are enforced, it is difficult for participants and voters not to accept the election results or the legitimacy of the newly elected representatives.”

ACE is not the only organization that is concerned about transparency. The Organization for Security and Co-operation in Europe’s (OSCE) Office for Democratic Institutions and Human Rights (ODIHR) is also focused on transparency through their efforts related to election monitoring and observation. Like the ACE Project, the OSCE/ODIHR has a strong interest in ensuring that elections are run in a free and fair manner; in fact, this organization monitored the 2007 Estonian Parliamentary Elections [OSCE07].

The rationale for transparency in elections is simple; when elections are not transparent, individuals may engage in some sort of fraud or electoral manipulation that cannot be observed. In addition, even if nothing nefarious happens, a lack of transparency creates a situation where government officials cannot answer questions about the election in a way that satisfies either political parties or the citizenry. Erin Peterson notes that transparency has been closely tied to the idea of accountability and legitimacy in both the public and private sectors because it provides the public with important information about how institutions function[9]. Other scholars have found that transparency, especially in the vote counting process and the ability of observers to follow the election and watch key actions, are critical to confidence in the election process [Hy08]. In evaluating the legitimacy of an election system, transparency is a key attribute in the overall evaluation of the electoral process [Hy08].

In evaluating legitimacy, there are key features to examine based on international principles[10]. In order to evaluate the Estonian electoral system with Internet voting, it is important to determine whether the system has legal legitimacy among the public, the government, third-party election monitors, and the electoral administrators that implement election. It is also important that there are procedures in place that facilitate election observation and electoral transparency.

[9] Pe07 cites the works of Be95; BO99; FS02; Mo98; PR96; and SL01 as leading scholars in the area of transparency.
[10] See HW08a and HW08b for a review of this literature.

Our review of the Estonian case utilizes these international norms as a framework for understanding the way in which the Estonian government fosters transparency and legitimacy in the electoral process. We begin our evaluation by considering whether the political process that allowed for Internet voting is viewed as legitimate and was developed in a transparent political process (i.e., one in which I-voting was not adopted in a politically-motivated fashion to introduce bias into the system). Second, we are interested in examining whether the voters themselves view the Internet voting system as legitimate and fair. Third, we consider the administrative environment in which Internet voting is implemented and whether that system promotes transparency. Fourth, we consider how Internet voting is observed and audited. A transparent system should be one that promotes openness and is viewed as legitimate; by using international norms for election transparency as a framework, we can see how well Estonia's system fares.

3 The Legitimacy of the Estonian I-voting System

The legitimacy of I-voting in Estonia comes from the fact that the nation has relatively strong political support and an excellent legal framework that provides for Internet-related government services generally, including I-voting [DM02, DM04; MMV06]. The backbone to the entire system is the Digital Signature Act (DSA) of 2000. This Act provides for Estonians to be able to authenticate themselves during online transactions, including I-voting, and to use a digital signature. In 2002, Estonia began providing its citizenry with an identity card that had two individual's digital certificates embedded in it. When a user inserts the card into a standard smart card reader affixed to a computer and then connects to the websites enabling different services via the Internet, the individual can then enter their first personal identification number (PIN1) and the user is authenticated and can access an array of governmental and private services online. In order to give electronic signature the second certificate is activated by giving PIN2. According to Administrative Procedure Act, public sector is obliged to accept digitally signed documents and a digital signature has the equal legal value as a handwritten signature.

The DSA links closely with the set of laws enacted in 2002 that allow for I-voting in various electoral settings: the Local Communities Election Act, European Parliamentary Election Act, and the Riigikogu Election Act. After significant amendments in 2005, these laws detail the manner in which I-voting is to be administered. The statutes detail when voters can cast ballots over the Internet, the use of the DSA in voter authentication, the process for allowing I-voters to cancel their vote using an early-vote paper ballot, reconciling voter registries so that I-voters cannot cast a ballot on election day, and the ballot reconciliation process for I-votes on election night. The strong authentication requirement for I-voters i.e. the usage of ID card, is also for mitigating the risk of vote selling. Forwarding one's ID card will compromise a person's identity in all transactions not only in elections.

Electoral laws were sponsored and supported by the Prime Minister and the Minister of Justice and continue to be supported by the Parliament. In addition, the Estonian ministries have been supporters in I-voting and have championed its success in talks around the world. The most controversial issue of guaranteeing secrecy of remote I-voting by allowing people to vote repeatedly is also supported by the Estonian Supreme Court, which has ruled that repeated I-voting is constitutional because the technological benefits outweigh any deficiencies. Specifically, the court stated that "the infringement of the right to equality and of uniformity, which the possibility of electronic voters to change their votes for unlimited number of times can be regarded as amounting to, is not sufficiently intensive to overweigh the aims of increasing the participation in elections and introducing new technological solutions."" [Court05]. If these laws were no longer deemed legitimate by either the political parties or the public, the Parliament would obviously be in a position to change them but there has been no reason to do so. No election results have been challenged during the I-voting elections and no parties have officially questioned the transparency of the process in the political or legal setting.

One reason why the system is deemed to be transparent is that the laws governing I-voting ensure that the Internet is but one way that voters can cast ballots in Estonia. Voters can also vote in person during the early voting period on a paper ballot or they can vote on a paper ballot in person on Election Day. Internet voters can use the early voting period to ensure that their vote was secret. On the early voting period the election law allows an I-voter to cast multiple I-votes, with only the last vote counted and included in the reconciled election totals. In addition, if an I-voter casts a paper ballot during the early voting period, no I-vote is counted, only the paper ballot. By re-voting, the voter who was illegitimately influenced is able to cast a new vote once the influence is gone. Thus, an I-voter has multiple means of ensuring that their vote counted is a secret, un-coerced vote.

The legal framework for the Estonian I-voting system provides the system with legitimacy because the decision to move to I-voting was made in an open, deliberative process. The government carefully considered the issues associated with I-voting and ensured that there was an appropriate set of legal mechanisms in place to fulfil this expectation. The timing of I-voting, concomitant with early voting, allows an I-voter the opportunity to cast a secret, un-coerced ballot.

4 Voter Legitimacy: Options for Dealing with Negative Effects of I-Voting

As was noted previously, the improper influence of remote voters by others is a theoretical but potentially significant problem, although such threats are tolerated with vote-by-mail in numerous jurisdictions. As Alvarez and Hall have noted, the threats that exist with I-voting are similar to the threats that exist in almost all other modes of voting [AH04, AH08]. In order to reduce the potential threat of coercion or a problem with a perceived loss of privacy in remote I-voting, reversible voting during the early voting period is allowed under Estonian electoral law.

If we consider the experience of voters in the two I-voting experiences, we see that there is little evidence of coercion or concerns about privacy, based on the behaviour of voters. The number of I-voters who decided to go to the polling station in order to replace their I-vote with a paper ballot has decreased from 0.3% in 2005 to 0.1% in 2007 (see Table 1). Also, the percentage of repeated votes compared to the total number of I-votes diminished accordingly from 3.8% to 2.5%. The small percentages of repeated votes as well as the significant increase of the total number of I-voters indicate that the confidence in the existing I-voting system has grown. These two statistics suggest that few voters have felt the need to use the various reversible voting mechanisms that exist to guard against coercion. However, it is valuable that the small percentage of voters who have used the system, for whatever reason, have had a system in place to allow them to change their vote and avoid this concern. Likewise, the reporting of these data by the Estonian government provides voters with confidence that their votes were reversed in the process and their replacement vote tabulated.

	Local elections 2005	Parliamentary elections 2007
Number of I-votes	9 681	31 064
Repeated I-votes	364	789
Number of I-voters	9 317	30 275
I-votes cancelled by paper ballot	30	32
I-votes counted	9 287	30 243
% of I-votes among total votes given	1,9%	5,4%
% of I-votes among total advance votes given	7,2%	17,6%
% of I-votes cast abroad (51 countries in 2007)	n.a	2 %

Table 1: Internet voting statistics of 2005 and 2007 elections [NEC2007].

In addition, we see a large growth in the percentage of voters who used the I-voting channel from 2005 to 2007. In its first use, 1.9% of voters used I-voting; in 2007, 5.4% used the system. In a survey of voters and non-voters in both elections, respondents who cast I-votes in 2005 reported having also I-voted in 2007. I-voters were very loyal to the technology, suggesting that their experience in 2005 convinced them of the system's effectiveness [TSB07]. By comparison, other voters were not loyal to their voting method; election day voters tended toward early voting and early voter to I-voting. In addition, there was some evidence that I-voting brought a small but potentially significant number of non-voters into the electoral process. This is important because studies in the United States have suggested that a lack of confidence in the electoral process can lead individuals to decide not to vote [AHL08]. Internet voting in Estonia seems to have the reverse effect, potentially drawing in some voters who previously did not participate in the electoral process. A survey of voters after the 2007 parliamentary elections found that 1 in 10 internet voters suggested that they might not have voted if the internet option had not been available [TSB07]. The contrast between America and Estonia can be seen here between the relatively low level of technology trust in the United States and the high I-government support in Estonia.

The Estonian government has also used simple methods to increase voter understanding of and confidence in the I-voting system in an attempt to overcome any concerns about the lack of transparency and complexity. In both elections in which I-voting has been used, prior to the voting period, the government allowed all individuals eligible to vote the opportunity to test out the I-voting system in order to encourage people to see how the system worked. This helped the voters detect any problems they might encounter before the real I-voting period started. In Estonia, the primary concerns among the country's election officials, outside observers, political parties, and citizens, relate to the cost and acquisition of the hardware and software needed to read an ID card on a personal computer, updating expired ID card certificates and the renewal of PIN codes needed for electronic use of the ID card. The government engaged in a nationwide pre-election information campaign to inform voters about these potential issues and to encourage voters to try the system before the voting period started. In 2007 elections, about 4,000 voters did test the system.

5 Transparent Election Administration

In addition to having voters test the system so that they would know how the electronic equipment worked during the voting period, there were also other issues about which the national election officials wanted to educate I-voters. Specifically, in order to raise the confidence of voters, they were informed that they should ensure that the file of the voting application had not been modified in transmission or intercepted by untrusted parties. This was done by explaining to voters how, once the live voting period had started for I-voting, they could verify the authenticity of the voting application. Before the start of the I-voting period for some operational systems, the election officials published information about the cryptographic hash functions that were used, and during voting period voters could examine the checksums.

As an additional element of transparency, the number of I-voters who had cast ballots was updated regularly on the I-voting website during the early voting period. This very simple process allowed the wider national audience, as well as the political parties, to know how many i-voters had voted and to determine if the trend in the number of i-voters casting ballots seemed reasonable. At the end people were also able to compare the number of I-voters with the number of I-votes counted. The transparency of the election process was not mere window-dressing on the part of either election officials or voters. One real example that illustrates that the importance of allowing voters and the political parties to monitor the I-voting should not be underestimated. As the i-voting system was closed at the end of the early voting period, the final number of I-voters disappeared from the I-voting website for a couple of minutes. This incident caused immediate and intense feedback from voters.

A high level of transparency is appealing because it provides the voters as much data as they need so that each voter is convinced that her vote has been correctly registered. One key question is to know how much information can be reflected back to the voter without creating other problems. For example, one possibility is to let the voter inspect the ballot as it is registered in the trusted part of an Internet voting system (analogous to checking the statement of account in Internet banking). The ballot can only be inspected, not modified [Sk06] and the possibility for inspection may give the voter even greater trust in the system.

This idea has been thoroughly discussed during the development process of the Estonian Internet voting system but the realization of it was postponed. Therefore, other methods were used in order to convince the voter. If the voter decided to replace the I-vote with a new one, he got a notification of an earlier recorded I-vote. A second option for verifying the correctness of electoral administration was offered on election day in the polling station of voter's residence, where the fact of an valid I-vote had to be reflected on the polling lists in order the prevent voting more than once.

The I-voting system actually provides I-voters with more assurance that their ballots were included in the final tabulation and were tallied accurately compared to the traditional paper ballot system. The I-voter has two mechanisms that could increase the confidence of voters. First, voters who use the I-voting mechanism know that there is no misinterpretation of their ballot by a third-party. They do not have to worry whether the polling place workers can read their writing on election night and properly count their ballot; by contrast, all I-votes were counted. Second, the voter can check acceptance of an electronic I-vote during the I-voting period or after the end of the advance poll as described earlier.

6 Transparency and Observation in Practice

In the case of Internet voting, observation is of particular importance for several reasons. First, the introduction of new technologies can influence public opinion with regard to the ability of the election process to produce honest, verifiable results. In Estonia the electoral administration enjoys broad confidence of the electorate. This confidence is reflected in the fact that, even with the implementation of this new voting mechanism, the interest of domestic observers in observing the Internet voting was quite modest in last elections. Second, the introduction of such a new technology can influence international opinion about Estonia. This interest is reflected in the high interest that international observers have had towards Estonian I-voting and their efforts to assess whether Estonian elections using I-voting are conducted in line with international standards for democratic elections, provide an opportunity to identify potential concerns, and enhance the integrity of the elections process not only for Estonian public opinion but internationally. Third, there are also theoretical concerns that, given the electronic nature of the voting, the system is inherently less transparent than is traditional precinct based balloting.

According to the Estonian electoral laws, all activities related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, counting and tabulation of results. Internet voting has been no different. All significant documents describing the I-voting system have been made available for all, including observers. In order to enhance the observers' knowledge about the system, political parties were invited to take part in a training course before each election in which I-voting was used. Besides political parties, auditors and other persons interested in the I-voting system also took part in the training. The training was followed by surveys of concrete procedures that were necessary for a set up of the I-voting system. Observers were invited also to a test of the counting process. However, few political parties exercised their opportunity to observe the I-voting procedures.

Throughout the I-voting observation period of one month, the main observation tool was the checking of the activities of electoral administrators against written documentation describing the necessary procedures. The key management function required extra attention, as the security and anonymity of I-votes was predicated on the encryption and decryption of votes. During counting event - the highlight of the election period - the management of the private key was demonstrated to observers. NEC mastered this key, and its members collegially could open the anonymous encrypted votes. The process of conducting the counting of ballots was all conducted with observers able to watch all ballot counting activities on large screens in the observation area. The process was fully narrated and observers were able to follow each step.

It is important that observers are deployed for a length of time necessary to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, the conclusions about the integrity of the system can not be made. In last elections of March 2007, I-voting procedures started several weeks before the elections day. Especially for casual foreign observers, the length of the observation period appeared to be a challenge. The OSCE did audit the 2007 elections and, in its report, it states that "election administration implemented the [Internet voting] system in a fully transparent manner, and appeared to take measures to safeguard the conduct of internet voting to the extent possible" [OSCE07].

The Estonian NEC has also been very supportive of analyses of its voting system by academic observers. In both 2005 and 2007, the NEC provided support to studies conducted by the Council of Europe that evaluated public confidence in the I-voting system. These two studies both found that there was a high level of public confidence in I-voting and provided an independent audit of public attitudes toward the I-voting system. Given the fact that transparency and confidence are not tangible but are attitudinal, these studies of public opinion in Estonia allowed the NEC and others involved in the elections to have additional knowledge that the I-voting system was effective and the procedures being used were acceptable to the public.

7 Validating the Voting Systems – Audit, Certification, Testing

The Estonian I-voting system was developed with the underlying principle being that all components of the system should be transparent for audit purposes. Procedures should be fully documented and critical procedures should be logged, audited, observed, and videotaped as they are conducted.

Specifically, during last elections, NEC has conducted audits on the source code and on the electoral procedures. A common requirement is that the source code of the voting system should be available for auditing. In Estonia, though, the code is not universally available but it can be audited if agreed to by the NEC. In order to rule out any manipulation by insiders, every election and audit by external auditing company had been ordered and it covered all of the technical and operational activities controlled by electoral committee. The audit was conducted by KPMG Baltics, which reviewed and monitored security sensitive aspects of the process continuously, such as updating the voters list, preparation of hardware and its installation, loading of election data, maintenance and renewal of election data and the process of counting the votes. The auditors' report about the 2007 Parliamentary election was released after all procedures, including the deletion of I-votes, were carried out. The report stated that the I-voting followed the rules described in the system's documentation and the integrity and confidentiality of the system were not endangered.

The I-voting system produces a wealth of system log information that can be used to monitor the work of the system thoroughly. In its different production functions, the I-voting system produces different logs on received, cancelled, and counted votes, also invalid and valid votes. The Audit Application enables to determine what happened to an I-vote given by a concrete person without revealing the voter's choice. These logs provide external auditors as well as observers with information that they can use to ensure that the system is working correctly.

The OSCE, in its report about the 2007 Parliamentary elections, recommended that, in addition to the audits of the process now conducted, all components of the system should be audited by an independent body in accordance with publicly available specifications, with all reports made public [OSCE07]. NEC has not published the audit reports referring to the contracts and given the consideration that publishing reports could make the system more vulnerable to attacks. In the future, the NEC should consider asking its auditors to produce both an internal audit report, intended for the NEC, and a report that can be made public, with certain information redacted.

In order to validate the electronic voting system, certification procedures could be established and other measures like testing and audits of different aspects should be taken. The Council of Europe has stated that it is necessary to promote the development of certification and accreditation schemes for e-voting systems in the member countries [CoE06]. A certification process will be very useful if there are a number of e-voting systems available. It might become very hard for any electoral authority to make sure a particular product is ready to be used, will operate correctly and will produce accurate, reliable results [Rec04].

Currently there is no domestic or international body that is ready to certify Estonian I-voting system. Estonia instead uses a system similar to that used in other countries, where a third-party audits the source code to ensure that the system operates as is specified. In addition to the audits discussed previously, system testing was also done on separate operation and functional components of the system in order to test the functionality and accuracy. Two weeks prior to the advance electronic voting period, the I-voting system was also tested by the public and contracted testers.

8 Conclusions

It is critical all election systems have fundamental safeguards for transparency in place because without them the public confidence necessary for legitimating elections cannot be ensured. Tools like observation, independent auditing, and system testing are suitable for assessing the actions of the electoral administrators. In addition, third party evaluations of public confidence in the process also serve to enhance our understanding about whether the public views the election with confidence and sees that the election administration was in fact transparent. These tools might not be easily accessible or of interest to the average person; however, it should be simple for those individuals who do want to participate.

The two Estonian I-voting experiences seem to prove that it is possible to solve the legal as well technological obstacles inherent for remote e-voting concerning the transparency of elections. The high degree of public confidence enjoyed by electoral administrators in last elections, as well as the fact that the legitimacy of the whole election process—including Internet voting—has not been questioned, strongly suggest that the elections have been carried out transparently. Moreover, the electoral administrators have provided procedural mechanisms that educate voters and the political parties about the process and allow each, through simple activities, to be an active participant in the election observation and evaluation process. The test voting process, the ability to re-vote, and the ability to determine that their vote was accepted all provide voters with a chance to evaluate and check the I-voting system.

In order to increase public awareness about IT security and teach people how to use the Internet safely, new initiatives, like public-private project “Computer Security 2009” and state’s Information Society Awareness Program have been started. The aim at further increaseing the use of e-services with due attention to security issues and application of ID-card, will most probably raise the popularity of Internet voting in the future. Based on researches success of Internet voting is clearly linked to the overall ICT awareness [TSB07]. Next elections using I-voting as an option will take place in the year 2009.

ICT has already dramatically changed the way elections are conducted in many countries, and it must be accepted that this process will go on and affect more and more countries. Even if Estonia is still the only one practicing Internet voting countrywide on legally binding elections, it could be a matter of time when people in other countries also overcome their native conservativeness against new solutions. To get experiences, the first step has to be taken and trust can be built only based on experiences. Insecurity is the part of every IT system, but in order to reduce the insecurity a lot can be done. And learning from experience is highly valuable in making the I-voting transparent and confident

References

[AHL08] Alvarez, R., Hall, T., Llewellyn, M.: Are Americans Confident Their Ballots Are Counted? Journal of Politics 2008 [Forthcoming].

[AH04] Alvarez, R., Hall, T.: Point, Click, and Vote: The Future of Internet Voting. Washington, DC. Brookings Press 2004.

[AH08] Alvarez, R., Hall, T.: Electronic Elections: The Perils and Promise of Digital Democracy. Princeton University Press 2008.

[Be95] Bell, A.: Constitutional Aspects. The International and Comparative Law Quarterly. Vol. 44, No. 3. (Jul., 1995), pp. 700-705.

[BO99] Bloomfield, R. and M. O'Hara.: Market Transparency: Who Wins and Who Loses? The Review of Financial Studies. Vol. 12, No. 1. (Spring, 1999), pp. 5-35.

[CoE06] Remmert, M.: E-Voting in Europe: Standards, policy practice, 2006.

[Court05] Decision of the Supreme Court of Estonia of Electronic Voting, http://www.nc.ee/klr/lahendid/tekst/RK/3-4-1-13-05.html.

[DM02] Drechsler, W, Madise, Ü.: "E-Voting in Estonia." Trames, 2002, 6(56/51), 3, 234-244.

[DM04] Drechsler, W., Madise, Ü.: Electronic Voting in Estonia. In: N. Kersting and H. Baldersheim (eds.) Electronic Voting and Democracy. A Comparative Analysis. Basingstoke: Palgrave Macmillan 2004, pp. 97-108.

[FS02] Faust, J., Svensson, E.O.: The Equilibrium Degree of Transparency and Control in Monetary Policy. Journal of Money, Credit and Banking, 2002, vol. 34, No. 2., pp. 520-539.

[HW08a] Hall, T., Wang, T.: Show Me the ID: International Norms and Fairness in Election Reforms. Public Integrity, 2008, 10, 2: pp. 97-111.

[HW08b] Hall, T., Wang, T.: Normative Principles for Evaluating Election Fraud. In Alvarez, R.M. Hall, T.E. and Hyde, S. (eds): Understanding, Detecting, and Preventing Election Fraud: Domestic and International Perspectives. Washington, D.C., Brookings Institution Press 2008.

[Hy08] Hyde, S.: How International Election Observers Detect and Deter Fraud. In Alvarez, R.M. Hall, T.E. and Hyde, S. (eds): Understanding, Detecting, and Preventing Election Fraud: Domestic and International Perspectives. Washington, D.C., Brookings Institution Press 2008.

[Ma07] Maaten, E.: Practicing Internet Voting in Estonia. In Baltic IT&T Review 2007, http://www.ebaltics.com/00704985?PHPSESSID=f5849c543bdc4a1b621bd4c73eb62fc0

[MMV06] Maaten, E., Madise, Ü., Vinkel, P.: Internet Voting at the Elections of Local Government Councils in October 2005. Report on Internet Voting to the National Election Committee, Tallinn 2006, http://www.vvk.ee/english/report2006.pdf.

[Mo98] Moncrieffe, J.M.: Reconceptualizing Political Accountability. International Political Science Review / Revue internationale de science politique 1998, Vol. 19, No. 4. (Oct.), pp. 387-406.

[NEC07] National Electoral Committee of Estonia: Parliamentary Elections 2007 – Statistics of e-voting, http://www.vvk.ee/english/Ivoting_stat_eng.pdf.

[OSCE07] OSCE/ODIHR Election Assessment Mission Report, Republic of Estonia, Parliamentary Elections, 4 March 2007, http://194.8.63.155/item/25385.html.

[PR96] Pagano, M., A. Roell.: Transparency and Liquidity: A Comparison of Auction and Dealer Markets with Informed Trading. The Journal of Finance, 1996,Vol. 51, No. 2, pp. 579-611.

[Pe07] Peterson, E.: Transparency In United States Election Law. Thesis Manuscript, University of Utah.

[Rec04] Recommendation No. R (2004) 11 of the Committee of Ministers to members states on E-Voting, http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec(2004)11_Eng_Evoting_and_Expl_Memo.pdf.

[SHN06] Skagestein, G., Vegard Haug, A.V., Nødtvedt, E., Rossebø, J.: How to create trust in electronic voting over an untrusted platform. In: Krimmer, R. (Ed.) Electronic Voting 2006, Bonn: Gesellschaft für Informatik 2006, pp. 107-116.

[SL01] Stirton, L., Lodge, M.: Transparency Mechanisms: Building Publicness into Public Services. Journal of Law and Society 2001, Vol. 28, No. 4., pp. 471-489.

[Tr06] Perspectives e-voting. Presentation made at the E-Voting Conference in Tallinn, October 2006, http://www.ega.ee/files/27.10.06_Michael_Remmert_e-haaletamise%20konv.pdf

[TSB07] Trechsel, A.H., Schwerdt, G., Breuer, F., Alvarez, M., Hall, T.: Report for Council of Europe - Internet voting in the March 2007 Parliamentary Elections in Estonia. http://www.coe.int/t/e/integrated_projects/democracy/EVoting/Report_Evoting_Estonia_for_the_CoE_2007.doc.

Session 2: Empirical Findings of E-Voting

Assessing the Impact of E-Voting Technologies on Electoral Outcomes: an Analysis of Buenos Aires' 2005 Congressional Election

Gabriel Katz[1*], R. Michael Alvarez[1], Ernesto Calvo[2], Marcelo Escolar[3], Julia Pomares[4]

[1]California Institute of Technology
[2]University of Houston
[3]Universidad de Buenos Aires
[4]London School of Economics
*corresponding author: gabriel@hss.caltech.edu

Abstract: Using data from an e-voting experiment conducted in the 2005 Congressional Election in Argentina, we estimate the effect of different e-voting technologies on the likelihood that citizens cast their vote for different parties for the National Congress and the Legislature of Buenos Aires. Our results indicate that voters are extremely receptive to the information cues provided by the different voting technologies and associated ballot designs, and that particular voting devices have a significant impact on voter choice, systematically favouring some parties to the detriment of others. We conclude that the choice of alternative electronic voting devices might have considerable effect on electoral outcomes in multi-party electoral systems.

1 Introduction

An increasing number of countries around the world have adopted electronic voting systems in national and local elections since the 1990s, and many others are conducting pilot projects [AH08]. While the academic literature has focused mainly on the reliability and accuracy of different electronic voting technologies [AH08], [St04], [AS05], only a few empirical studies have directly examined the effect of different voting technologies on election outcomes [Wa04], [CM07], [HW07]. Empirical studies have even been fewer in multiparty electoral systems, where with a larger number of parties and candidates on a ballot, voters might be more responsive to readily available information and thus may resort to different cues in order to identify and distinguish the various electoral options and to select their preferred choice [RS06].

In this paper, we analyze how different voting technologies influence voters' choice and election outcomes in multiparty races, examining evidence from a voting pilot conducted in the 2005 congressional election in Buenos Aires, Argentina, in which four e-vote prototypes were tested. We show that voters alter their electoral behaviour and their vote choice in response to different e-vote technologies, and that this might translate into different electoral outcomes across voting devices. Our main findings are in line with the results of [CSP07], in the sense that 'technology matters,' and that different voting technologies and associated ballot designs might have substantive effects on election results in multi-party electoral systems.

2 The E-Voting Experiment in Buenos Aires' 2005 Election

Voters in the congressional election held in Buenos Aires in October 2005, elected National representatives and State legislators using a party-list paper ballot system that included candidates for all offices[11]. Seats were allocated using a PR-D'Hont formula with closed party lists of magnitude 13 for representatives and 30 for legislators. Thirty parties presented candidate lists for National representatives, while forty one parties presented lists for the state legislature. Three parties captured approximately 66% of the valid votes in the election of national representatives and 64% in the election of state legislators: President Kirchner's *Frente para la Victoria* (FPV), the center-left opposition party *Alianza para una Republica de Iguales* (ARI), and the center-right *Propuesta Republicana* (PRO)[12]. The campaign for national representatives was very intense, with high spending in support of the candidacies of Rafael Bielsa (FPV), Elisa Carrio (ARI), and Mauricio Macri (PRO). By contrast, candidates to the local legislature spent almost no money during the campaign [CSP07].

The e-pilot was conducted in 41 precincts randomly distributed throughout the city and included 14,800 participants. After voting in the official election, participants in each precinct were asked to participate in a non-binding election in which they were randomly assigned to one of four possible voting devices and were asked to vote a list of national deputies and a list of local legislators. Because the experiment was carried out in a single electoral district, with participants in each precinct being randomly assigned to the different voting devices and facing similar menus of party choices, we expect no correlation between the characteristics of the district or the election and voters' behaviour[13].

[11] The description of the e-vote pilot borrows from [CSP07].

[12] The vote-shares of ARI, FPV and PRO in the election of national representatives (state legislators) were 22.0% (20.8%), 20.5% (19.5%) and 34.1% (33.2%), respectively. If blank ballots are excluded, the vote share of these three parties comes close to 70%.

[13] Organizational problems prevented the testing of all the prototypes in all the precincts, as originally planned. While Prototypes 1 and 2 were tested in all the precincts, Prototype 3 was tested in 40 precincts, and Prototype 4 in only 17. Although we do not expect this to have resulted in serious imbalance between the participants assigned to the different prototypes, we take this problem into account in the analysis below.

After the vote, participants were asked to complete two surveys. The first survey was a short self-administered survey (six questions) conducted with 13,830 respondents. Half of the questions were identical across prototypes, dealing with general perceptions about their e-vote experience. The remaining questions tested usability issues specific to each device. A fourth of the participants also answered a longer exit poll. This survey provided information about the voters' political sophistication, their familiarity with technology, their patterns of political participation, and their opinions and attitudes towards electronic voting.

The four voting devices tested in the pilot were developed with the institutional process of Argentina in mind. *Prototype 1* was a direct recording electronic (*DRE*) design with two separate modules. A screen in the first module allowed voters to review the lists of candidates, and a numerical keypad was used to register the vote. Voters would insert a "smart card" into the first module and use the keypad to navigate through screens to cast their ballots. When done, they removed their smart card, moved to a second module, and again inserted their smart card, automatically recording their vote. *Prototype 2* was a touch-screen *DRE* machine with a voter verifiable paper trail. After activating the system with their plastic "smart card" voters could scroll and select party lists directly by tapping onto the screen. When done with their ballot, a paper audit trail would be generated underneath a glass screen. If the voter affirmed that that indeed was how she wanted her vote to be cast, the paper audit trail fell into a bin and the voter was done; if not, the paper audit trail was rejected and the voter was allowed to cast the ballot again. *Prototype 3* was an optical scan (OS) prototype located inside a voting booth. The voter picked paper ballots for the party list she wished to support inside the booth, inserted those ballots into a rolling scanner that displayed the selected party on the prototype's screen, and would then proceed to confirm her selection. This prototype required separate ballots for each race, allowing direct comparison of the marks that identify a party across races. Finally, *Prototype 4* was an optical scan device with a single ballot listing all the parties running candidates for office in the two congressional. The voter marked her preferences for each race with a pencil and introduced the ballot into a scanner; the ballot would then fall into a ballot box. In all prototypes, participants voted for National representatives first and State legislators second.

An important difference between the DRE and OS prototypes was the way in which voters were required to search for their preferred candidates. In the DRE prototypes, party labels were randomly rotated on the screen and, because of space restrictions, a limited number of labels were displayed on each screen. Two and three screens were required to display party labels for national representatives and state legislators in *Prototype 1*, while three and four screens were required in *Prototype 2*. The placement of the party labels rotated randomly for each voter, preventing order effect biases from favouring the same party. In the case of *Prototype 3*, poll workers sorted the paper ballots numerically[14]. According to the information obtained from the polling place workers, however, ballots rapidly mixed in the voting booth, complicating the search for the voters' preferred ballots. Finally, in *Prototype 4*, party names were listed by their official list number in increasing order. The non-random ordering of parties may have increased the likelihood of order effects but it also facilitated the recognition of the same party across races.

A second relevant difference among the prototypes was how voters accessed information about candidates and parties. The first prototype displayed 15 party names on each screen, including the list number and party logo information. In order to view the list of candidates, however, the voter needed to enter the three-digit party number. If the voter did not know the name of the party, she would need to access each list until finding a recognizable candidate name. *Prototype 2*, on the other hand, displayed the name of the first candidate under the party label, together with the number and logo information. The complete list of candidates was then displayed on a second navigation level. Parties with prominent first candidates (such as the pro-Kirchner Rafael Bielsa from the FPV or Mauricio Macri of the center-right PRO) were readily identified by voters[15]. However, very little information about the party name or number was recalled when casting the legislative vote. Hence, while voters faced fewer problems in recognizing their preferred choice for national representative, they could not use such information when choosing state legislators.

Different information was available to voters using the optical scan systems. Ballot papers for *Prototype 3* included all the relevant information, such as party name, party logo, identification number, and the complete list of candidates for each race. The only difficulty in identifying the preferred choice, therefore, was in finding the correct paper ballot. In *Prototype 4*, a booklet provided voters with all the party information; the ballot introduced in the rolling scanner listed only the party name, number and logo. The main characteristics of the four prototypes tested in the experiment are summarized in this paper's supplementary materials (Appendix I).

[14] When registering the candidates running for an election, each party is assigned a list number. Candidates and Parties advertise this number during the campaign, together with the party and candidate's name.
[15] Bielsa was President Kirchner's Foreign Relations Minister at that time, while Macri is a famous businessman and was the president of one of the most famous soccer teams in Argentina.

3 A First Look at the Impact of Different E-Voting Technologies

The survey data lets us examine how voters interacted with each prototype and how the different voting technologies and the associated ballot designs affected voters' electoral choice. Table 1 presents data about which ballot features participants used to identify their preferred candidates. Nearly half of the voters cast their ballot based on the name of the party, followed by the name of the first candidate. The name of the party was particularly important for those participants using *Prototype 4*, and was less so for those using *Prototype 3*. Also, the name of the first candidate was more relevant for those assigned to *Prototype 2*, while participants using *Prototype 1* were less likely to use it as a voting cue, using more frequently the party number instead. This is consistent with the characteristics of the ballot designs associated with the different prototypes: the name of the first candidate figured prominently on the computer screen in the case of the second prototype, while voters using *Prototype 1* could access the candidates' names only after entering each party's number in the keypad. We found a statistically significant relationship between the information used by respondents to identify their preferred candidate and the voting technology used (p-value = 0.08).[16]

Information used as voting cue	Prototype 1 (%)	Prototype 2 (%)	Prototype 3 (%)	Prototype 4 (%)	All prototypes (%)
Party name	51.4	51.0	44.3	53.4	49.4
First candidate's name	33.3	50.1	47.1	45.0	44.2
Party Logo	27.3	30.3	22.4	7.4	25.8
Party number	35.4	21.0	19.9	28.6	25.3
Other features	4.1	2.7	7.5	6.4	4.6
N	879	1,158	858	189	3,084

Table 1: How voters found their preferred candidates[17]

Table 2, in turn, reports the percentage of participants who stated they were not able to vote for their preferred candidate for each of the prototypes, sorted by education and political information levels[18].

[16] Given that respondents could use several ballot features to identify their preferred choice, the assumption of independence among units required by standard tests of independence is violated. Thus, we used the bootstrap resampling method proposed in [LS98] to test for the association between voting cue and prototype.

[17] Table entries are the percentage of respondents in each prototype that used each of the ballot features to identify their preferred candidates. Since participants could use several of the ballot features as voting cues, percentages do not necessarily sum to 100 rows across.

[18] Both surveys included the question: "Were you able to vote for your preferred party/candidate?" Political information was computed as the average of respondents' number of correct answers to three questions asking them the names of the ministers of economy, education and health.

The survey data indicates that education significantly affected the ability of the participants to vote for their preferred party while only 3.8% of voters with college education were unable to cast a vote for their preferred option; this figure was almost 2.6 times higher for those with high school education or lower. The difference in the proportions between the two groups is statistically significant, with a 95% confidence interval of [0.04, 0.08]. Although less educated voters experienced more difficulties in all of the prototypes tested, the gap between participants with college education and the rest was much smaller for *Prototype 2*, suggesting that this device imposed lower barriers on less educated voters. The p-value of Woolf's test for homogeneity across prototypes is 0.001 [Wo55], indicating that there are considerable differences across voting technologies regarding the difficulties experienced by less educated participants.

When examining the data by political information levels, again, *Prototype 2* seems to have been more effective in enabling voters with null or low information levels to vote for their preferred choice. *Prototype 3*, in contrast, exhibits the higher rates of reported voting problems for all levels of political information. The Cochran-Armitage Trend Test [AG02] provides evidence of a modestly negative linear relationship between political information and reported voting problems (two-sided p-value = 0.1), but this is only statistically significant (at the 0.01 level) for *Prototype 1*. Overall, almost 90% of the voters were able to vote for their preferred party; *Prototype 2* exhibited the highest rate of success (93.9%), while *Prototype 3* had the lowest score (82.6%).

Variable	Prototype 1 (%)	Prototype 2 (%)	Prototype 3 (%)	Prototype 4 (%)	All prototypes (%)
Education					
College	3.0	2.7	6.5	3.6	3.8
Secondary or lower	12.6	4.5	13.6	12.9	9.8
N	3,175	3,873	2,743	887	10,678
Non-response rates	21.4	18.4	28.2	27.5	22.8
Political information					
Null	9.9	3.4	11.4	0.0	7.3
Low	7.3	4.1	11.7	2.4	6.9
Medium	1.7	4.3	11.5	7.3	5.7
High	3.0	3.8	10.5	3.8	5.4
N	835	1,108	823	185	2,951
Non-response rates	5.0	4.3	4.1	2.1	4.3

Table 2: Percentage of voters who could not vote for their preferred candidate[19]

[19] Table entries are the percentage of respondents in each prototype that were not able to cast a vote for their preferred candidate, among all respondents belonging to each row-category assigned to that prototype. The data on education levels was taken from the short self-administered survey, while the data on political information was obtained from the longer exit poll.

The fact that the four prototypes imposed different information demands on the participants and seem to have influenced the cues they used to identify the candidates, suggests that the e-voting devices could have had systematic effects on electoral outcomes. For instance, parties with more visible candidates should have fared relatively better among voters using *Prototype 2*, and those with more recognizable names/logos might have benefited from the ballot design and screen display in the DRE devices. Figure 1 explores this issue further, plotting the means and 95% confidence intervals of the vote-shares of the parties in the election of National representatives and State legislators under each prototype[20,21.] For all the prototypes tested, each of the three majority parties, *Alianza para una Republica de Iguales* (ARI), *Frente para la Victoria* (FPV) and *Propuesta Republicana* (PRO), exhibited higher vote-shares in the first election, jointly obtaining 65% of the total vote cast for the parties competing in the election of National representatives. In contrast, minority parties gathered almost 50% of the vote in the less visibility race for State legislators. However, there are considerable variations in the support for the different parties across prototypes. The support for minority parties in both races was substantially higher under *Prototype 3*, reaching 48.7% in the election of National representatives and 55.7% in the election for the local legislature. In contrast, their vote-share was the lowest under Prototype 4, with 36.4% and 41.6% respectively. The support for the largest parties also varied across prototypes. For the four prototypes tested, the vote-share of ARI, FPV and PRO in the in the National (Local) election was 21.0% (18.2%), 15.6% (12.6%) and 22.6% (19.9%), respectively. However, the three large parties fared considerably better under the two DRE devices than under *Prototype 3*. We used bootstrapped Kolmogorov-Smirnov tests to examine the differences in each party's average support between pairs of prototypes [Ab02]. We found statistically significant differences at the usual confidence levels between the average vote-shares of FPV and PRO under *Prototypes 1* and *2* and their support under *Prototype 3* in both congressional races, as well as between the support for ARI under *Prototypes 1* and *3* in the national election. There are also significant differences in the support for the smaller parties under *Prototype 3* and each of the other prototypes in the two elections analyzed[22].

[20] Vote-shares are expressed as percentages of the total number of votes cast for the competing parties in both races, excluding blank and null votes. Although Prototype 3 had a higher rate of blank ballots than the other e-voting devices [CEP07], the results regarding the relative support for the different parties remain virtually unchanged when including blank ballots in the analysis.

[21] Note that, while ARI's vote-shares in the two experimental elections were similar to those in the official elections, the support for FPV and PRO was lower and the vote for the smaller parties was higher in the pilot, compared to the actual elections.

[22] See Appendix II of the paper's supplementary materials for details.

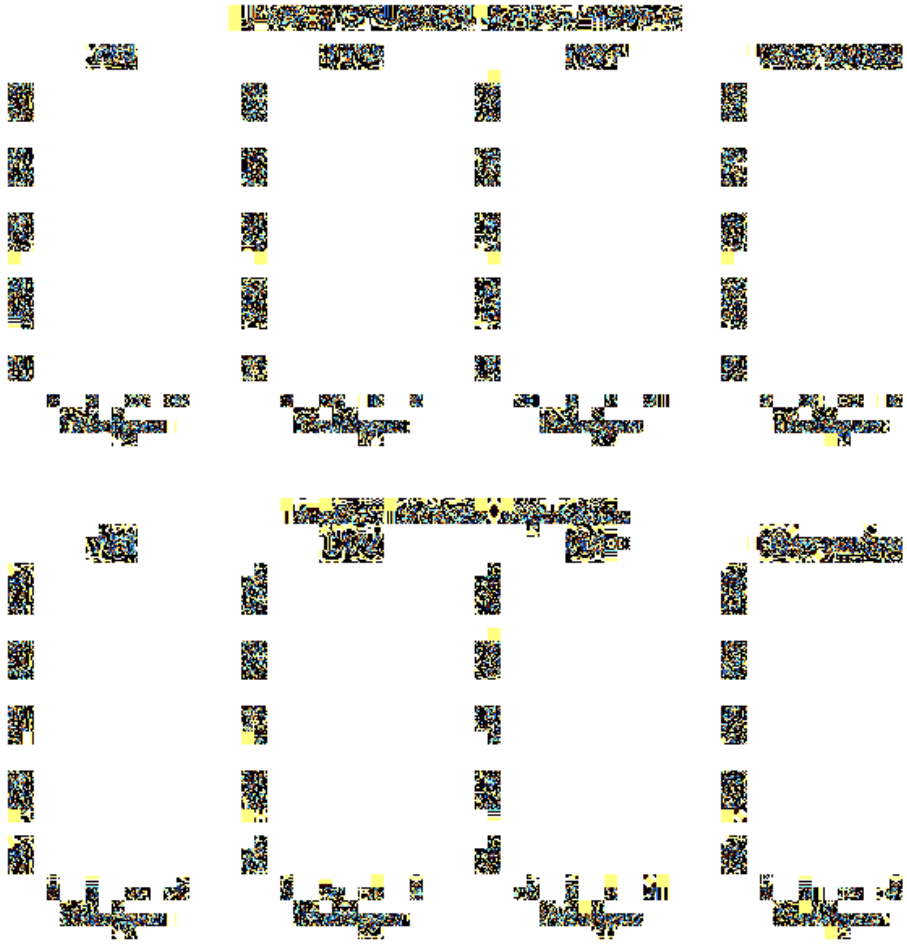


Figure 1: Distribution of the support for the parties under each prototype[23]

[23] The thick horizontal lines correspond to the median vote-shares of the parties under each prototype. The rectangles correspond to the 50% interval, and the outer thin lines to the 95% intervals.

4 Estimating the Effect of E-Voting Technologies on Election Outcomes

While the data presented in the previous section reveals some interesting differences in voters' electoral behavior across voting devices, it does not allow us to assess the impact of the different technologies and ballot designs on the voter choice after accounting for the effect of socio-demographic and attitudinal variables. Controlling for these predictors might be relevant in order to estimate the causal effect of the e-voting devices on voters' choice and election outcomes [GH07], given that not all of the four prototypes were used in all the districts analyzed[24].

As our data includes the individual level votes for all the participants in the pilot, we can analyze the aggregate electoral and survey data from 128 voting stations defined by crossing each of the precincts with the e-voting devices[25]. Our dependent variable is the vote-share of ARI, FPV, PRO and Other parties in the election for National representatives and State legislators in each of the voting stations, where the category "Other parties" comprises all the remaining parties in both races[26]. The independent variables used in the analysis are defined at the voting station level and include: the mean Education level; the mean level of *Political Information; Interest in politics*; the mean level of participants' *Use of Technology*; *Perceived Difficulty of E-Voting*; and four variables measuring the percentage of participants who found their preferred party searching by *Party Name*, by *Party Logo*, by *Party Number*, or by *Candidate Name*. Additional details and descriptive statistics for these variables are provided in Appendix III of this paper's supplementary materials.

In order to estimate the causal effect of different voting technologies on the expected support for the parties competing in 2005, we implemented a multinomial-logistic model for the multinomial probabilities of support for ARI, FPV and PRO, with "Other parties" as the baseline category [Co05]. The probabilities of support for the parties are modelled as functions of the voting station covariates described above. In addition, in order to account for the cluster sampling scheme used in the experiment and to allow for unobserved heterogeneity across voting stations and for potential correlation in the election results across prototypes and precincts, we include zero-mean random effects for the two non-nested factors [Co05], [GH07]. The model was fit by MCMC Gibbs sampling methods [CS92]. The main advantage of using Bayesian estimation is that it allows obtaining arbitrarily precise approximations to the posterior densities, without relying on large-sample theory [Ja04].

[24] See footnote 3.
[25] Although the individual vote variable can be retrieved from each prototype's logs, privacy considerations prevented us from linking the individual vote with the individual survey data. Combining the information from the logs and the surveys, we have data from 128 out of the 139 possible voting stations, after dropping 924 individual observations with missing values from our analysis.
[26] "Other parties" includes 26 smaller parties in the election for National representatives and 37 parties in the election for the State Legislature.

In order to evaluate the model fit, we used posterior predictive simulations to assess the model's ability to reproduce the overdispersion present in the data, comparing the Pearson statistic computed from the observed data with that computed using replicates sampled from the model [Co05]. Additional details about the model specification, the estimation procedure and robustness checks are provided in Appendix IV of the supplementary materials.

5 Empirical Results

Table 3 reports the posterior means and standard deviations for the fixed effects for the two elections under analysis. The model satisfactorily replicates the overdispersion in the data, with values of $P\left(\chi^2_{\text{Rep}} > \chi^2_{Obs}\right)$ close to 0.5 for both elections [Co05].[27]

Parameter	Election of National representatives			Election of State legislators		
	ARI	FPV	PRO	ARI	FPV	PRO
Education	0.10 (0.14)	-0.23*** (0.09)	0.29** (0.12)	0.14 (0.10)	-0.23** (0.11)	0.29* (0.15)
Political information	0.54* (0.32)	0.27 (0.33)	-0.36 (0.34)	0.70** (0.30)	-0.01 (0.33)	-0.09 (0.33)
Interest in Politics	-0.15 (0.19)	0.41* (0.21)	0.24 (0.20)	-0.09 (0.19)	0.44* (0.22)	0.51*** (0.19)
Use of Technology	0.05 (0.16)	0.10 (0.17)	0.25 (0.17)	0.01 (0.16)	0.33* (0.18)	0.22 (0.16)
Assessment of E-Voting	0.19 (0.43)	0.34 (0.35)	0.19 (0.36)	0.36 (0.40)	0.05 (0.50)	-0.16 (0.37)
Search by Party Name	-0.54** (0.26)	-0.18 (0.28)	-0.44* (0.26)	-0.11 (0.27)	-0.59** (0.31)	-0.29 (0.27)
Search by Party Logo	0.01 (0.31)	0.02 (0.34)	0.24 (0.33)	-0.05 (0.32)	0.18 (0.35)	0.45 (0.34)
Search by Party Number	-0.06 (0.32)	0.77** (0.35)	0.43 (0.34)	-0.21 (0.33)	0.52 (0.39)	0.12 (0.33)
Search by Candidate Name	-0.39 (0.25)	-0.06 (0.25)	-0.73*** (0.27)	-0.07 (0.24)	0.05 (0.28)	-0.47* (0.27)
Intercept	-1.13 (1.44)	-1.03 (0.68)	-2.73** (1.09)	-2.48** (1.05)	-0.77 (1.15)	-3.44** (1.31)
N	128			128		
$P\left(\chi^2_{\text{Rep}} > \chi^2_{Obs}\right)$	0.42			0.57		

Table 3: Estimated posterior means and standard deviations for the fixed effects
(Standard deviation in parenthesis; significance levels: *** 0.01, ** 0.05, *0.1)

[27] χ^2_{Obs} is the usual Pearson statistic computed from the observed data, and χ^2_{Rep} is using the replicates sampled from the model. See Appendix IV in the supplementary materials.

The results in Table 3 reveal some interesting differences regarding the effect of several covariates on the relative support for the three largest parties. For instance, in the two elections analyzed, the votes for *Propuesta Republicana* (PRO) increased in voting stations with higher average levels of education, while they decreased for *Frente para la Victoria* (FPV). In contrast, higher average levels of political interest were associated with higher support for FPV. This result is consistent with prior research that emphasizes class and education effects among non-Peronist voters [CM04]. Regarding the effect of the different information cues used by participants when casting their vote, the support for FPV in the more visible race increased with the percentage of voters relying on the official party number. On the other hand, the vote for ARI and PRO was negatively related to the percentage of participants using the name of the party in the election for National representatives, while there is a negative relationship between *Search by Party Name* and the support for FPV in the less visible election. The vote for PRO was also negatively associated by the percentage of voters basing their choice on the first candidate's name in both congressional elections.

The main focus of our analysis, however, lies in the effect of the different voting technologies on the support for the competing parties across elections. Figure 2 presents the posterior means and confidence intervals of the prototype effects for each of the parties in both elections.

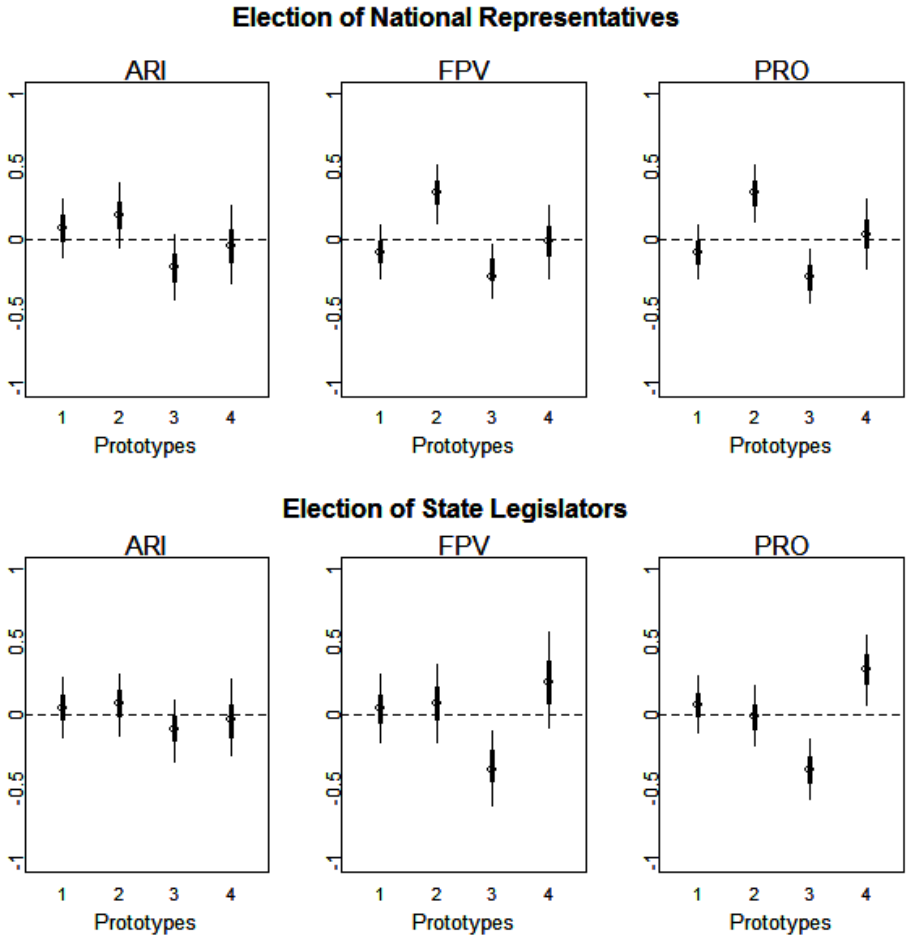


Figure 2: Prototype random coefficients for both congressional elections[28]

[28] The center dots correspond to the point estimates of the prototype effects, the thicker lines to the 50% confidence interval, and the thinner lines to the 90% confidence interval.

These results indicate that different voting devices have potential influences on electoral outcomes after controlling for socio-demographic and behavioural variables. The effect of the voting technologies and the associated ballot designs varied considerably across parties and races. For instance, while the Optical Scan device with separate ballots (*Prototype 3*) had a significantly negative effect on the votes for FPV and PRO in both congressional elections, the touch-screen DRE device (*Prototype 2*) had the opposite effect, raising the support for FPV and PRO in the election for national representatives, although not in the election for state legislators. As mentioned above, the name of the first candidate of each party figured prominently on the screen of *Prototype 2*, and more than half of the participants using this device cast their vote based on this information. Hence, a possible interpretation of this result is that, while the first candidates of FPV and PRO, Bielsa and Macri, were renowned figures who were easily identifiable by voters, participants generally did not recognize the candidates running for the local legislature of any of the competing parties [CEP07]. Thus, the relative advantage obtained by FPV and PRO in the more salient election disappeared in the less visible race. Interestingly, however, the results reported in Table 3 show that the percentage of respondents using the first candidate's name had no systematic effect on the support for FPV in either of the races, while it had a negative impact on the vote for PRO. This indicates that the prototype-effects might be capturing additional sources of variability in the dependent variables, beyond that explained by the aggregate survey data.

Table 4 complements the information presented in Figure 2, reporting the mean posterior and 50% and 90% confidence intervals of the pairwise differences in the probabilities of supporting each party across prototypes. After controlling for other factors, the support for the largest parties tends to be higher for the two DRE devices than for *Prototype 3*, although the differences between *Prototype 1* and *3* are not statistically significant at the usual confidence levels. In contrast, in the cases of FPV and PRO, there are significant differences between their support for *Prototypes 2* and *3*: the touch-screen DRE device leads to an increase of 3.8 and 6.3 percentage points in their vote-shares, respectively, in the election for National representatives, and of 2.7 and 5.3 percentage points in the election for state legislators; these differences are significant at the 0.01 level. As shown in Figure 2, in the more visible race, these differences stem both from an increase in the support for FPV and PRO induced by *Prototype 2* and a reduction of their support for *Prototype 3*. In contrasts, the results in the election for state legislators are entirely driven by the higher support for the smaller parties under the OS device with separate ballots. In fact, the relative support for the smaller parties tends to be consistently higher with *Prototype 3* in both races: in the national representative election, the vote-share of the minor parties is 11 percentage points higher under *Prototype 3 vis a vis Prototype 2*, while in the state legislature election their vote with this prototype is systematically higher when compared against all the other voting devices. Also, in the national election, the relative support for the smaller parties is lower with *Prototype 2* than *Prototype 1*. Hence, in the more visible race, the touch-screen DRE device consistently favours the parties with more renowned candidates, to the detriment of the smaller ones.

	Pairwise comparisons	π^{ARI}	π^{FPV}	π^{PRO}	π^{OTHER}
Election of National representatives	Prototypes 1-2	2.1 (-4.2, 8.7)	-3.6 (-8.4, 1.0)	-5.2 (-10.9, 0.4)	6.6 (0.8, 12.4)
	Prototypes 1-3	3.4 (-3.2, 9.9)	0.2 (-4.0, 4.4)	1.2 (-4.6, 2.1)	-4.8 (-10.8, 1.7)
	Prototypes 1-4	2.9 (-0.4, 6.0)	-1.0 (-4.3, 1.9)	-2.4 (-6.0, 1.0)	0.5 (-3.6, 4.3)
	Prototypes 2-3	1.3 (-0.5, 3.3)	3.8 (2.1, 5.7)	6.3 (4.4, 8.3)	-11.0 (-13.7, -9.2)
	Prototypes 2-4	0.7 (-6.9, 8.0)	2.6 (-3.3, 8.3)	2.7 (-4.2, 9.4)	-6.1 (-13.0, 1.0)
	Prototypes 3-4	-0.5 (-7.7, 6.5)	-1.2 (-6.3, 4.9)	-3.6 (-9.8, 2.4)	5.3 (-2.1, 13.4)
Election of State legislators	Prototypes 1-2	-0.6 (-5.4, 5.1)	-0.55 (-5.5, 4.6)	1.5 (-4.2, 6.9)	-0.4 (-7.7, 6.5)
	Prototypes 1-3	-0.2 (-5.3, 5.2)	2.7 (-1.5, 7.4)	5.3 (-0.1, 10.4)	-7.8 (-15.1, -0.8)
	Prototypes 1-4	2.5 (-0.5, 5.4)	-1.7 (-5.0, 1.4)	-4.0 (-7.8, -0.3)	3.1 (-0.9, 7.2)
	Prototypes 2-3	0.4 (-1.4, 2.2)	3.3 (1.8, 4.9)	3.8 (1.9, 5.7)	-7.5 (-9.8, -5.1)
	Prototypes 2-4	3.1 (-2.8, 8.7)	-1.1 (-7.8, 5.2)	-5.5 (-12.2, 1.5)	3.5 (-4.6, 12.3)
	Prototypes 3-4	2.7 (-3.0, 8.0)	-4.4 (-10.6, 1.1)	-9.3 (-15.6, -3.1)	11.0 (2.8, 19.5)

Table 4: Pairwise differences in the probability of support for each party across prototypes in percentage points (90% confidence intervals in parenthesis)

These results provide strong evidence in support of the hypothesis that alternative voting technologies may have substantive influence on the support for different parties. The relevant question thus becomes: how would the election outcomes vary under different voting technologies? In order to answer this question, we estimate the expected electoral outcome assuming only one prototype had been used in each voting-station, while holding all the remaining variables constant. Table 5 reports the expected election outcomes in both races for each of the four prototypes and compares them to the actual results in the experiment.

The evidence indicates that different voting technologies would in fact have led to quite different election results. For instance, if *Prototype 1* had been used in all voting stations, ARI would have had the highest expected support in the election for national representatives, rather than the actual winner, PRO. ARI would also have had the highest expected support in the election for state legislators under *Prototype 3*. In contrast, the vote-shares of PRO and FPV in the national election would have been maximized under *Prototype 2*, increasing their support at the expense of ARI and, especially, of the smallest parties. In the less visible race, however, the advantage enjoyed by PRO and FPV under the touch-screen DRE device would have virtually vanished. Finally, the expected support for minor parties in both races would have increased by almost 6 percentage points under *Prototype 3* with respect to the actual results in the experiment. Thus, the choice among different e-voting technologies could have had substantive effects on the election results.

	ARI	FPV	PRO	Other Parties
Election of N. Representatives				
Prototype 1	22.77	14.52	21.59	41.12
Prototype 2	20.64	18.13	26.74	34.49
Prototype 3	19.36	14.33	20.40	45.91
Prototype 4	19.89	15.52	23.99	40.60
Actual outcome in the experiment	21.03	15.58	23.16	40.24
Election of S. Legislators				
Prototype 1	18.00	12.97	21.87	47.16
Prototype 2	18.57	13.52	20.38	47.53
Prototype 3	18.16	10.25	16.59	55.00
Prototype 4	15.47	14.64	25.84	44.05
Actual outcome in the experiment	18.04	12.31	20.43	49.22

Table 5: Expected and actual election outcomes in percentage points

6 Concluding Remarks

Multiparty races impose substantial demands on voters, who have to gather enough information to be able to distinguish between the positions of the different parties before the elections and to identify their preferred choice at the polls. Using data from a large-scale e-vote experiment in Buenos Aires, we present the first study on the impact of different electronic voting systems on election outcomes in multi-party races. Our results indicate that different devices have considerable influence on the relative support for different parties across races, after controlling for relevant socio-demographic and behavioural predictors. In contrast to studies on this topic examining two-party elections in the U.S., most of which have found that the impact of alternative voting technologies on election outcomes is quite small [CS07], [HW07], our findings show that this effect might be large enough to potentially affect the election results. In this sense, our results are in line with the findings of [RS06], indicating that amount and the form in which information is presented to voters by different e-voting technologies might have a considerable influence on voting behavior in multi-party elections.

The evidence presented in this paper is particularly significant in view of the increasing trend towards electronic voting and the growing number of countries moving from traditional paper ballots to electronic voting systems. In many of these countries, political parties have repeatedly expressed concerns about the possibility of being systematically disadvantaged by the new voting technologies[29]. Our results suggest that this might actually be the case, rather than just a myth fuelled by politicians, and raises the possibility that some voting technologies may in fact shape the electoral outcomes, rather than merely recording voters' preferred choices.

References

[Ab02] Abadie, A.: "Bootstrap Test for Distributional Treatment Effect in Instrumental Variable Models". Journal of the American Statistical Association, 97(457), 2002, pp. 284-292.

[Ag02] Agresti, A.:Categorical Data Analysis. New Jersey: John Wiley & Sons. 2002.

[AH08] Alvarez, R.; Hall, T.: Electronic Elections: The Perils and Promises of Digital Democracy. Princeton, NJ: Princeton University Press, 2008.

[AS05] Ansolabehre, S.; Stewart, C.: "Residual Votes Attributable to Technology". Journal of Politics, 67(2), 2005, pp. 365-389.

[CEP07] Calvo, E.; Escolar, M.; Pomares, J.: "Ballot Design and Split Ticket Voting in Multiparty Systems: experimental evidence on information effects and vote choice." Unpublished manuscript, 2007.

[CM04] Calvo, E.; Murillo, M.: "Who Delivers? Partisan Clients in the Argentine Electoral Market." American Journal of Political Science, 48(4), 2004, pp. 742-757.

[CM07] Card, D.; Moretti, E.: "Does Voting Technology Affect Election Outcomes? Touch-screen Voting and the 2004 Presidential Election". Review of Economics and Statistics, 89 (4), 2007, pp. 660-673.

[CG92] Casella, G.; George, E.: "Explaining the Gibbs Sampler". The American Statistician, 46(3), 1992, pp. 167-174.

[Co05] Congdon, P.: Bayesian Models for Categorical Data. New York: John Wiley & Sons, 2005.

[GH07] Gelman, A.; Hill, J.: Data Analysis Using Regression and Multilevel / Hierarchical Models. New York: Cambridge University Press, 2007.

[HW07] Herron, M.; Wand, J.: "Assessing partisan bias in voting technology: The case of the 2004 New Hampshire recount". Electoral Studies, 26(2), 2007, pp. 247-261.

[Ja04] Jackman, S.: "Bayesian Analysis for Political Research". Annual Review of Political Science, 7, 2004, pp. 483-505.

[LS98] Loughin, T.; Scherer, P.: "Testing for Association in Contingency Tables with Multiple Column Responses". Biometrics, 54(2), 1998, pp. 630-637.

[RS06] Reynolds, A.; Steenbergen, M.: "How the world votes: the political consequences of ballot design, innovation and manipulation." Electoral Studies, 25(3), 2006, pp. 570-598.

[S04] Stewart, C.: "The Reliability of Electronic Voting Machines in Georgia". Working Paper 20, Caltech/MIT Voting Technology Project, 2004.

[Wa04] Wand, J.: "Evaluating Voting Technologies: 2004 New Hampshire Democratic Primary. Technical Report, Stanford University, 2004.

[Wo55] Wolf, B.: "On estimating the relation between blood group and disease." Annals of Human Genetics, 19, 1955, pp. 251-253.

[29] For instance, several French parties expressed such concerns during the 2007 Presidential election, the first time electronic voting machines were used for a presidential election in the country (Le Figaro, 04/18/2007).

Assessing Internet Voting as an Early Voting Reform in the United States

Alicia Kolar Prevost

American University
4400 Massachusetts Avenue NW
Washington, DC20016
Alicia.prevost@american.edu

Abstract: Recent research on convenience voting reforms in the United States has found that programs designed to make voting easier have not succeeded in boosting turnout, and have even had the unintended consequence of exacerbating the demographic biases that already exist in the electorate by encouraging votes among those who were most likely to vote anyway but who were inconvenienced by going to the polls on election day. Using public voting records and a unique dataset of Internet voters in the 2004 Michigan Democratic Presidential primary, this paper offers new evidence that Internet voting benefits two groups of people: young voters and people who vote infrequently. Like previous research on voting reforms, I also find evidence that Internet voting does not draw new voters into the electorate. I discuss the implications of these findings for the future of early voting reforms in general and Internet voting in particular.

1 Introduction

Americans routinely use the Internet for banking, commerce, social networking, and even paying taxes, but they have not been able to use the Internet for voting in elections for public office. At a time when Internet use is widespread and voting systems are being reassessed in nearly every state, and when Internet voting has been successfully tested in European countries at the local and even national level, why has Internet voting not been introduced in state administered elections in the US? Although state and local election administrators have not embarked on tests of Internet voting, state political parties have used Internet voting in two binding state-wide elections. These trials, held in 2000 in Arizona and 2004 in Michigan, can provide important information about the feasibility of Internet voting in future elections in the US. Before state election administrators can plan online voting trials, we must have a better understanding of the online elections that have already occurred in the US. This paper offers a better understanding of how Internet voting affects turnout among different demographic groups.

Recent studies of voting reforms have found that programs designed to make voting easier have had only small positive effects on turnout and have had the unintended consequence of exacerbating the demographic biases that already exist in the electorate [Be05; Tr04]. Convenience voting reforms such as vote-by-mail, no-excuse absentee voting, and in-person early voting have been shown to encourage votes among those voters who were most likely to cast a ballot anyway but were inconvenienced by having to go to the polls on election day. Internet voting is the newest innovation among these early voting reforms. However, there have been few opportunities to study Internet voting as an early voting reform in the United States. Findings from academic studies of Internet voting in Arizona in 2000 and Michigan in 2004 have been mixed on the effect Internet voting has on turnout among certain demographic groups [AN01; PS08].

Using public voting records and a unique dataset of individuals who participated in the 2004 Michigan Democratic Presidential primary, this paper examines the claims that Internet voting specifically and early voting reforms in general may only benefit those who were most likely to vote anyway. This research builds on previous studies of the effects of Internet voting as an early voting reform by offering an examination of voters at the individual level and incorporating voting history as an indicator of future voting behavior. I find that young people and people who vote infrequently benefit most from Internet voting. I also find that income is positively related to voting online, but race and education were not significant predictors of voting on the Internet.

This research adds to the body of knowledge on voting behavior by introducing new evidence on the effects of Internet voting as an early voting reform. This paper also incorporates the use of state voter files as an alternative to more traditional data sources for studying the effects of voting reforms on voter turnout. Similar research that uses public voting records includes Berinsky, Burns and Traugott [BBT01], in which the authors obtain individual vote history and confirm self-reported voting behavior from county records for a group of survey respondents. Public voting archives are readily available in most states, and are used regularly by political operatives, but seem to be rarely used by political scientists. Since the effects of voting reforms are often very small, it may be necessary to examine these reforms at the individual level, as Berinsky, Burns and Traugott argue [BBT01].

I begin with a review of the research on early voting reforms in general and the limited trails of online voting in the US. I then summarize the details of the unique dataset that I employ, including information about the 2004 Michigan Democratic primary, and describe the methods that I will use to evaluate Internet voting. Finally, I present the results of a multinomial logit regression model and discuss the implications of these findings for the future of Internet voting as an early voting reform.

2 Literature Review

2.1 Poor Marks for Voting Reforms

In recent years, political science research on reforms to make voting easier has been nearly unanimous in concluding that the reforms have not met their stated goals of increasing turnout and improving the representativeness of the electorate. Paul Gronke's overview of voting reforms argues that scholarly consensus has been reached on this point: "Early voting does not increase turnout by bringing new voters into the system. What it does is encourage regular voters to participate in lower intensity contests that they might otherwise skip" [Gr04]. Berinksy [Be05] and Traugott [Tr04] offer similar reviews of the political science literature on voting reforms with the same conclusion: that voting reforms have not achieved the goals that the reformers had in mind, and in fact the demographic representativeness of the electorate is actually worsened by easy voting reforms since "more of the same" voters – that is, highly educated, older, and richer voters – are even more likely to turn out using easy voting methods.

Berinsky [Be05] reviews the literature on voting reforms and concludes that they have had "perverse consequences" in that they have encouraged the people who were most likely to vote anyway (those who have higher incomes and are more educated) but were inconvenienced by going to a polling place on election day. Traugott [Tr04] argues that electoral reform has failed because it has not achieved the goals of substantial increases in turnout or greater socioeconomic diversity in the electorate. These findings are important because they show that groups who have always been underrepresented in the electorate – the poor, people without college degrees, and young adults – may become an even smaller percentage of the electorate, as easy voting reforms encourage more voters with higher incomes and more education to turn out, and mail balloting encourages more older voters to turn out. In addition, these findings might also bolster the arguments of policy makers who are opposed to expanding early voting options. Given the potential implications of these findings for policy makers and election administrators, it is important that analyses of voting reforms be conducted with the best evidence available and at the lowest level of aggregation possible in order to make inferences about the effects on individual voters. However, much of the empirical research on voting reforms has relied on evidence that might not be generalizable to individual voters. Previous studies have used survey data [NR01], exit polls [SG97], and aggregate data [AN01; Gi02]; all of which are problematic for making generalizations about individual voters. Although these studies have contributed important findings about the effects of early voting reforms, it is important to recognize the possible limitations of using aggregate data or unverified survey responses to make public policy decisions. Telephone surveys are increasingly unreliable because of the high no-response rate, and respondents tend to over-report turnout [TK79]. Exit polls only survey voters (by definition they leave out the non-voters who are not at the polls), and aggregating voter turnout data at high levels makes it difficult to make inferences about individual voters.

Studies of Internet voting use self-reported telephone survey responses [So01], or turnout aggregated at the county level [Gi02; AN01], which is a high level of aggregation and therefore not an accurate estimator of individual-level information. One of the strongest arguments against Internet voting is that it is biased against racial and ethnic minorities and citizens of lower socioeconomic status, since these groups have less access to the Internet. This claim has largely been supported by the existing academic literature on Internet voting, including the finding that the decrease in turnout was five times as great for non-white voters in the Internet voting election in Arizona [AN01]. However, the authors of that study use data and demographic variables (including race) aggregated at the county level. Since there are only 15 counties in the state of Arizona, this is a particularly high level of aggregation. Another study of Internet voting that uses individual level information about voters in the 2004 Michigan primary found that race was not a strong predictor of choosing Internet over mail voting, but it was a factor in the choice of applying to vote early [PS08].

The analysis conducted in this paper extends the research of Prevost and Schaffner [PS08], which examined the pool of voters who participated in the 2004 Michigan Democratic primary to see if there were differences in the demographic characteristics of those who voted on the Internet, by mail, or in-person. Prevost and Schaffner [PS08] found that voters in predominately African American zip codes were somewhat less likely to vote on the Internet than voters in predominately white zip codes, but not by margins as large as some critics of Internet voting suggested. The authors also found that young people were most likely to take advantage of Internet voting, while older voters were more likely to take advantage of voting by mail.

2.2 Individual Voting History and the Likelihood of Voting

State voter files can show the relationship between voting history and the use of easy voting methods. The theory that infrequent or first time voters can be enticed into the electorate by easy voting reforms can be tested empirically using public voting records. Berinksy, Burns, and Traugott develop a duration model to see if individual vote history has an effect on whether voters will participate in Oregon's vote-by-mail system [BBT01]. They find that voting-by-mail encourages occasional voters who are older, well educated, and those with higher levels of interest in the campaign. They also find that habitual non-voters are not drawn into the electorate by the easy vote-by-mail system.

Given that voter history has an effect on future voting behavior, Berinsky [Be05] proposes a two-part conception of the electorate, in which he considers both the stimulation of new or infrequent voters and the retention of other voters from election to election. He contends that electoral reforms will have a greater effect on the retention of voters than on the stimulation of new voters. Berinsky reasons that electoral reforms "increase the propensity of likely voters to consistently turnout by smoothing over the idiosyncrasies that cause engaged citizens to sometimes miss casting their votes in particular elections" [Be05: 477]. He suggests that to properly observe the effects of voting reforms on the composition of the electorate, we should analyze individual-level data over time to see if easy voting methods are used by regular voters (retention) or infrequent voters (stimulation). However, the only research he cites that uses individual-level data over time is a study of voting by mail in Oregon [BBT01].

Other empirical research supports the claim that those who have voted previously are more likely to vote in the future. Green et al [GGS03] find that voting in one election substantially increases the likelihood of voting in a subsequent election. The authors find voter history to have a greater effect than education and age in predicting whether an individual will turn out to vote. Using a randomized field experiment, they find that voting in 1998 increased the probability of voting in 1999 by 46.7 percentage points [GGS03: 547]. These findings suggest that vote history is an important variable in any model predicting voting behavior, but it has rarely been used in political science studies of voting behavior. Two exceptions where individual voting history has been used are Plutzer [Pl02] and Berinsky, Burns and Traugott [BBT01]. Using panel data spanning several decades, Plutzer finds that voting (and non-voting) is "habitual" – once a person starts voting she is likely to continue doing so [Pl02]. Using individual level voting history from public voting records, I analyze the effects of voting history on the propensity to use Internet voting as an early voting method.

3 Description of the 2004 Michigan Democratic Presidential Primary

The 2004 Democratic presidential nominating contest in Michigan has been called a caucus, a firehouse primary, and a party-run primary. The Democratic National Committee (DNC) officially defined it as a party-run primary, because it had many features of a primary, including an option for absentee voting, so it is referred to as a primary in this paper. The contest had some features of a caucus, including the fact that ballots cast were not secret. This feature allowed the Michigan Democratic Party (MDP), which administered the election, to circumvent many of the security concerns associated with Internet voting, since it allowed each voter to be assigned a unique identification and PIN number. In order to participate in the party-run primary, an individual could either apply for an absentee ballot or vote in person on election day. The absentee ballot application could be accessed on the MDP website, and several presidential campaigns also distributed them to supporters. The application could then be completed online, or printed and sent by mail or fax to the MDP. Once the application was received by MDP staff, it was checked against the state voter file for accuracy, so a person applying for an absentee ballot had to be a registered voter in the state. Alternatively, a person could decide on election day to vote in person at a caucus location without having taken any prior action.

In many ways, the Michigan Internet ballot was much like a traditional absentee ballot that a voter would send in a secrecy envelope to prevent election workers from seeing for whom a particular individual is voting. Media reports of the Michigan primary did not mention voters being concerned with privacy violations. It may be the case that voters who choose to vote absentee have come to accept that there is a possibility that an election worker will see their vote choice, and that is an acceptable cost given the benefit of being able to vote early or from home. 162,929 voters participated in the 2004 Michigan Democratic primary. 28.4% voted by Internet, 14.5% voted by traditional mail-in absentee, and 57.1% voted in-person at a caucus location on election day.

Michigan does not require a voter to declare a party affiliation when registering to vote. One implication of this is that the state has an open primary system – a voter can take a ballot for either party's primary, which means that Republicans can vote in Democratic primaries, and vice versa. This violates the rules of the Democratic National Committee, and so the Democratic party in Michigan has been forced to administer party-run primaries or caucuses for its presidential nominating contests.

4 Data and Methods

Two datasets serve as the empirical evidence for this analysis: the Michigan Qualified Voter File and turnout data from the 2004 Michigan Democratic Primary. The Michigan Voter File is publicly available from the Michigan Secretary of State. It contains individual-level information about the voting behavior of each of the approximately 7 million voters who are currently registered in the state, including name, address, gender, date of birth, and voting history for every state administered election. However, since the 2004 Democratic Primary was a party-run election, which was administered by the state Democratic party, voter history information for this election is not included on the state voter file.

Turnout data from the 2004 Michigan Democratic primary was provided by the MDP. It contains individual level-information for the approximately 162,000 voters who participated, including name, address, and choice of voting method: Internet, mail, or in-person. Ideally, the data from the 2004 Michigan Democratic primary would be compared to only Democrats on the state voter file, in order to make inferences about who participated in the 2004 Caucus and who was eligible to participate (since only Democrats were supposed to participate, according to MDP guidelines for voting in the primary, although a small number of self-identified Republicans and independents participated). However, since there is no party affiliation on the state voter file, there is no easy way to determine which voters are Democrats. To account for this, and to simulate a measure of party affiliation, I include a control variable in the model that measures the vote for Gore in 2000 by each voter's state house district (adjusted for the 2002 round of redistricting).

The full state voter file contains close to seven million voters, which was too large a dataset for any computer or statistical package in my department to handle. To overcome the lack of computing power, I generated a random sample of one million voters from the state voter file. Although the accuracy of the analysis might be marginally better if I were able to examine all of the 162,000 voters in the Michigan primary in the context of all eligible or likely voters in the state, a sample of one million is still many times larger than any other similar study of the effects of voting reforms. After merging the turnout data from the 2004 Democratic primary with the sample, there are 16,906 voters in the sample who participated in the 2004 primary. Table 1 includes summary statistics of the sample. The distribution of choice of voting method in the 2004 primary among voters in the sample is similar to the distribution of choice of voting methods among the entire population of primary voters.

Variable	Frequency	% of sample
2004 Michigan Democratic Primary [1]	16,906	1.7
In-person	9,181	0.94
Internet	4,972	0.51
Mail	2,753	0.28
Gender [2]		
Women	514,813	53.6
Men	446,590	46.4
Age [2]		
18-35	296,103	30.8
36-50	306,693	32.0
51-65	214,634	22.3
66 and over	139,766	14.5
Education [3]		
0-25% college degree in zip code	487,500	50.71
26-50% college degree in zip code	389,583	40.52
51-75% college degree in zip code	75,963	7.90
76% or more college degree in zip code	8,444	0.88
Race [3]		
0-25% Black in zip code	823,502	85.66
26-50% Black in zip code	34,769	3.62
51-75% Black in zip code	31,649	3.29
76% or more Black in zip code	67,603	7.03
N = 961,403 [4]		

Table 1: Descriptive Statistics for Random Sample of One Million Voters taken from the Michigan Qualified Voter File

[1]2004 Michigan Democratic Primary participation data is from the Michigan Democratic Party.

[2]Gender and age variables are from the Michigan Qualified Voter File.

[3]Education and race variables are from the 2000 US Census, aggregated at the zip code level and assigned to each voter according to the voter's zip code.

[4]Final sample size is less than one million because some observations were dropped due to missing demographic data.

The individual-level data provided by the Michigan voter file and the MDP include each voter's name, address, zip code, date of birth, gender, voting history in state-run elections, and whether and by what method they participated in the 2004 primary. The demographic variables I am interested in are not easily available at the individual level. As a substitute for individual-level indicators of race, income, and education, I collected Census data aggregated at the zip code level, and assigned a measure to each voter based on their zip code of residence. Although aggregating at the zip code level is not a perfect substitute for individual-level measures, which are often available with survey data, the zip-code level is a relatively small level of aggregation compared to congressional district level or county level that have been used in other studies of voter turnout. The zip-code level has been used regularly in health research [GBN96] and it may also be a particularly good substitute in Michigan, which has been noted for its high level of racial segregation [DK00]. Still, it is important to highlight the point that the measures for race, education, and income in this study are aggregate level measures and should not be interpreted as substitutes for individual-level measures. Future extensions of this research could include Census data at a lower level of aggregation, such as the block level, since the dataset includes each voter's full address. This could add to the validity of the findings on the relationship between demographic characteristics and the use of Internet voting.

Instead of using a duration model to explain the relationship between voting history and the effectiveness of early voting reforms, as Berinsky, Burns and Traugott do [BBT01], this paper operationalizes voting history as a series of dummy variables. Table 2 summarizes the characteristics of each category of voting history.

	In-Person	**Internet**	**Mail**	**Abstain**
Nonvoter (voted in no previous elections since 1998)	1,079 (61)	464 (26)	216 (13)	423,374
Infrequent voter (voted in 1 general but no primaries)	7,766 (54)	4,273 (30)	2,432 (17)	402,568
Occasional voter (voted in at least 1 primary)	6,786 (54)	3,542 (28)	2,197 (18)	239,571
Regular voter (voted in last 3 elections)	5,733 (54)	2,986 (28)	1,943 (18)	160,342
Absentee voter (voted absentee in at least one election since 1998)	3,126 (46)	2,025 (30)	1,573 (23)	152,790

Source: Vote history is from the Michigan Qualified Voter File and choice of voting method (In-Person, Internet, or Mail) is from the Michigan Democratic Party.
Note: Number in parentheses is the percent of people participating in the 2004 Michigan Democratic Primary who voted by each method.

Table 2: Voting History by Choice of Voting Method in the 2004 Michigan Democratic Presidential Primary

As shown in table 2, a “nonvoter” in this analysis is someone who did not vote in any of the following elections; the 1998 primary and general election, the 2000 primary and general election, and the 2002 primary and general election. An “infrequent” voter is defined as someone who voted in one general election but no primaries. An “occasional” voter is someone who voted in at least one primary election, and a “regular” voter is someone who voted in each of the most previous three elections before the 2004 primary.

The dependent variable in the turnout model is the decision to vote in the 2004 Democratic caucus, either by Internet, mail, in-person on election day, or to abstain. Since it is a categorical dependent variable with no particular order to the categories, multinomial logit is the appropriate estimator. The independent variables of interest are voting history, age, gender, education, income, and race. Based on the findings of Alvarez and Nagler [AN01] I expect to find that as the percentage of white residents increases in a zip code, the likelihood of voting by Internet should also increase. I also expect that as median income and percent of residents with a college degree increases, the percentage of Internet voters should increase. As the age of the voter increases, I expect the likelihood to vote by Internet to decrease and the likelihood to vote by mail to increase.

Based on the findings of Gerber et al [GGS03], I expect regular voters to be more likely to participate in the 2004 primary, and that regular voters will be more likely to vote by early voting methods. Based on the findings of Berinsky, Burns and Traugott [BBT01] I expect to find that either infrequent or occasional voters will be the most likely to take advantage of Internet and mail voting, but that nonvoters will not take advantage of these easy voting methods, either because they are habitual non-voters, because they have not been mobilized by parties or candidates [RH93; Ol96], or because they did not have the foresight to apply for an absentee ballot [PS08].

5 Results

	Entire Random Sample of 1 million voters taken from the Michigan Voter File (N=961,403)						Voters in sample who participated in the 2004 Michigan Democratic Primary (N=16,906)			
	In Person vs. not voting		*Internet vs. not voting*		*Mail vs. not voting*		*Internet vs. in person*		*Mail vs. in person*	
Age of Voter[1]	.023*	(.001)	.013*	(.002)	.041*	(.003)	-.036**	(.003)	.025*	(.004)
Median Income[2]	-.014*	(.001)	-.003	(.001)	-.008*	(.001)	.013*	(.001)	.007*	(.002)
Percent College Educated[2]	.034*	(.002)	.038	(.001)	.029*	(.004)	.001	(.003)	.005	(.004)
Percent Black[2]	.003*	(.001)	-.0002	(.001)	.003	(.002)	-.003	(.002)	-.001	(.002)
Female[1]	.046**	(.021)	.146*	(.029)	.138*	(.039)	.120*	(.036)	.210*	(.045)
2000 Gore Vote[3]	1.63*	(.103)	1.72*	(.130)	1.56*	(.182)	.196	(.188)	.032	(.232)
Non-voter[4]	.476*	(.066)	-.109	(.083)	.177	(.125)	-.586*	(.106)	-.482*	(.142)
Infrequent voter[4]	2.51*	(.124)	2.61*	(.165)	2.01*	(.255)	.719*	(.213)	-.652**	(.304)
Occasional voter[4]	.52*	(.032)	1.39*	(.038)	1.56*	(.061)	-.133*	(.051)	.034	(.069)
Regular Voter (suppressed category)[4]										
Age X infrequent	-.018*	(.002)	-.029*	(.002)	-.017*	(.005)	-.020*	(.003)	.001	(.004)
Education X infrequent	-.008*	(.001)	-.001	(.002)	.002	(.004)	.006	(.003)	.009**	(.004)
Black X infrequent	-.008	(.002)	-.003	(.001)	-.001	(.002)	-.004**	(.002)	.000	(.002)
Constant	-.786*	(.089)	-9.22*	(.172)	-11.2*	(.259)	-.759*	(.222)	-2.73*	(.309)
Pseudo R^2	0.126						.048			

*p<.01 **p<.05

Note: 2004 Michigan Democratic Primary participation data is from the Michigan Democratic Party.

Table 3: Likelihood of voting in the 2004 Democratic caucus by Internet, mail, or in-person, compared to not voting – Multinomial Logit Regression Coefficients and Standard Errors

[1]Gender and age variables are from the Michigan Qualified Voter File.
[2]Education and race variables are from the 2000 US Census, aggregated at the zip code level and assigned to each voter according to the voter's zip code.
[3]2000 Presidential vote by State House District provided by Brian F. Schaffner.
[4]Voting history is from the Michigan Qualified Voter File. "Nonvoter" is someone who did not participate in any elections archived on the voter file since 1998; "Infrequent voter" is someone who participated in one general election but no primaries since 1998; "Occasional voter" is someone who participated in at least one primary election; and "Regular voter" is someone who participated in each of the last three state-wide elections before the 2004 primary.

Table 3 displays the results of two multinomial logit models. The first model includes the entire sample of one million voters; the second includes only the voters in the sample who participated in the 2004 Michigan primary. The first model uses "did not vote" as the base comparison category, since a large majority of voters in the full sample did not participate in the 2004 primary. The second model uses "voted in person" as the base category, since the majority of participants in the 2004 primary voted in person on election day.

In both models, the effects of age, income, gender, and all categories of voting history are significant at the .01 level. The interpretation of the findings that follows will focus on the second model, since I am mostly interested in voters who participated in the 2004 primary. As expected, the median income in a voter's zip code is significant and positively related to voting early. As income increases, the likelihood of voting early either by Internet or mail increases. The relationship between income and the likelihood of voting by Internet, mail, or in person, holding other variables in the model at their means, is displayed in Figure 1.

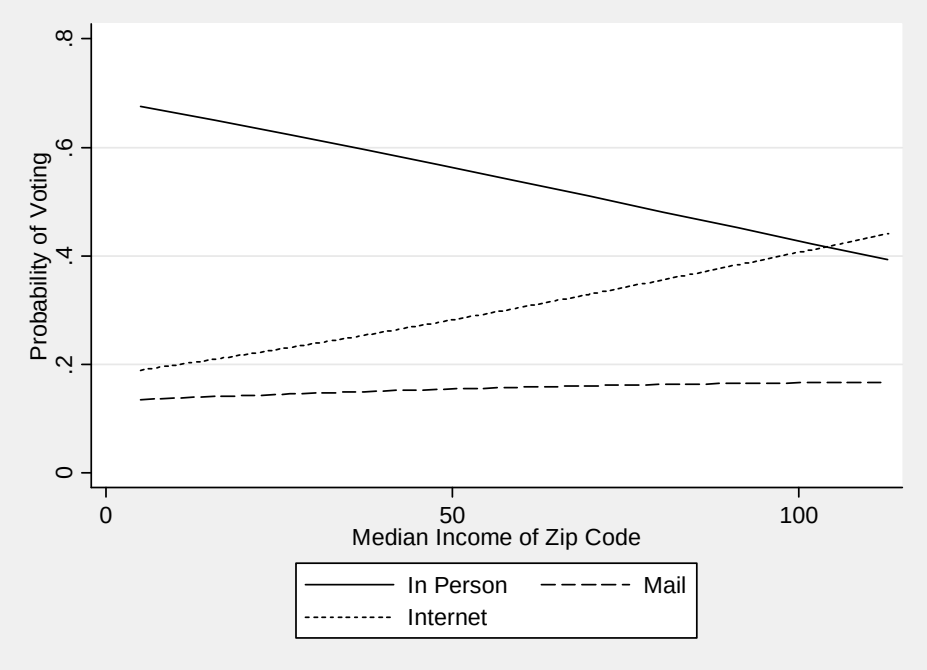


Figure 1: Probability of Voting by Internet, Mail, or In Person by the Median Income in the Voter's Zip Code

Also as expected, as a voter's age increases, he is more likely to choose voting by mail and less likely to choose Internet voting. This result is shown in Figure 2. As a voter's age increases, the likelihood of choosing to vote by mail increases substantially, while the likelihood of voting by Internet or in person decreases at a more gradual rate. The effect of age on the likelihood to vote by Internet may not be surprising to young people, who are probably the to most comfortable out any age group with using the Internet, but it is important for the study of early voting reforms. Other studies of early voting reforms, especially voting by mail, have found that older voters are more likely to benefit from early voting reforms. This research shows that young voters benefit from the option to vote on the Internet.

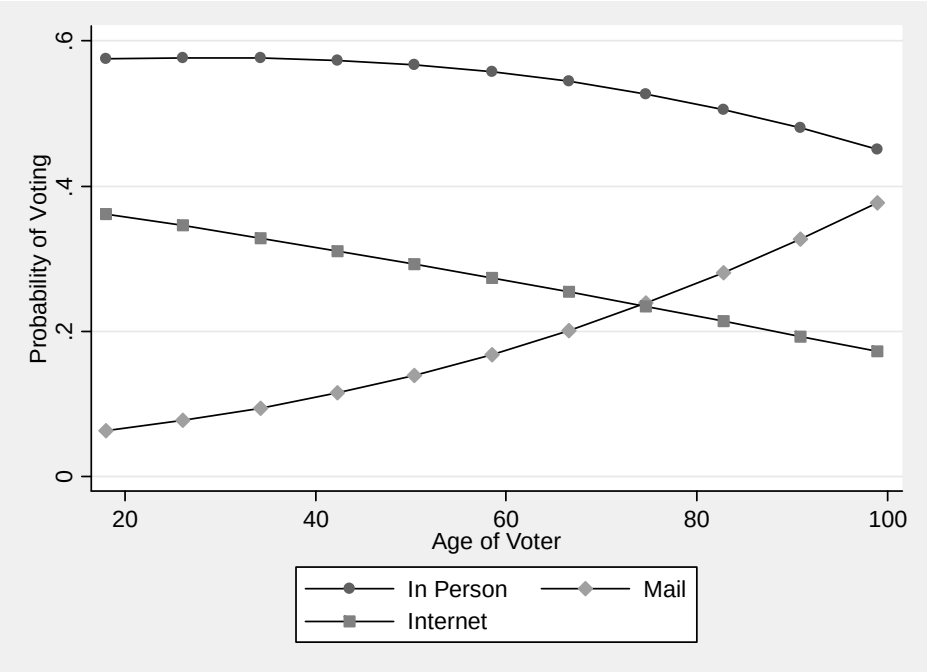


Figure 2: Probability of Voting by Internet, Mail, or In-Person by Age of Voter

The dummy variables for nonvoter, infrequent voter, and occasional voter are statistically significant at the .01 level in both models (regular voter is the suppressed category). As expected, being designated as a "nonvoter" was strongly and negatively related to voting on the Internet or by mail in the second model. Being an "infrequent" voter (one who voted in one general election but no primaries) was strongly and positively related to voting on the Internet, but strongly and negatively related to voting by mail, when controlling for other factors in the model. On the other hand, being an "occasional" voter (one who had voted in at least one primary) was positively related to voting by mail but negatively related to voting by Internet, controlling for other factors in the model. These findings are similar to those of Berinsky, Burns, and Traugott [BBT01], who found that individuals who voted sporadically were more likely to benefit from Oregon's vote-by-mail program. This model goes further to show that there is a difference between levels of frequency of voting. Infrequent voters were more likely to benefit from Internet voting, but occasional voters were more likely to benefit from mail voting. Figure 3 shows the predicted probabilities across the different categories of vote history for low and high values of a voter's age.

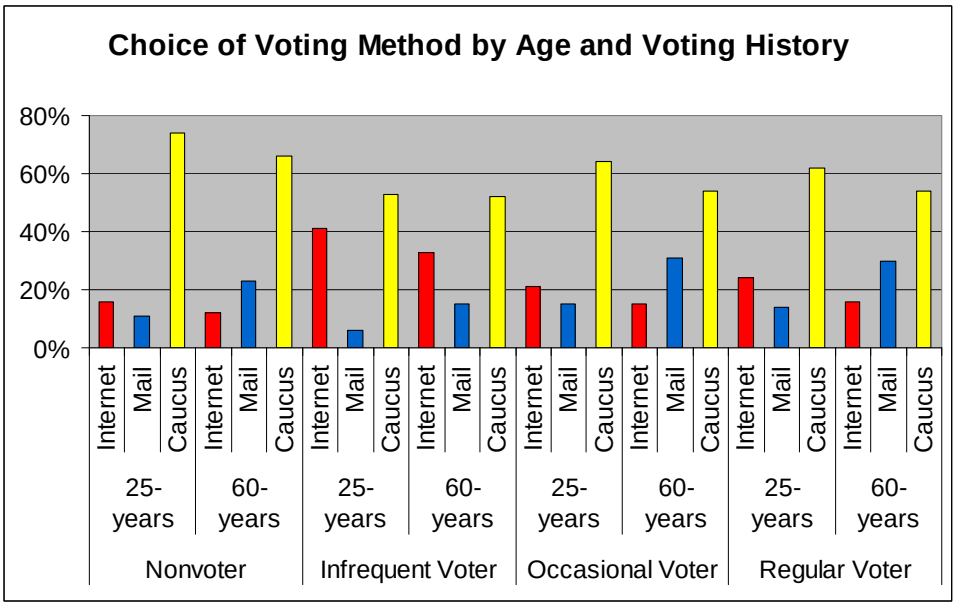


Figure 3: Predicting Choice of Voting Method for Voters Who Participated in the 2004 Michigan Democratic Primary, by Voter's Age and Individual Voting History

Younger voters in almost every category of voting history were more likely than older voters to choose Internet voting, and older voters were more likely to choose mail voting in almost every category. The only category in which both younger and older voters were more likely to choose Internet voting was for infrequent voters. For infrequent voters, 25 year olds were 41% likely to vote on the Internet and only 6% likely to vote by mail, and 60 year olds were 33% likely to vote by Internet and 15% likely to vote by mail. Although I expected to find that young voters would be more likely to choose Internet voting, I did not expect older voters to choose Internet voting over mail voting. This unexpected finding suggests that for future applications of this research, the composition of the voting history categories should be tested for robustness. The limits of time and computing power prevented this research from testing any additional models. It is also clear from Figure 2 that voting in person was the most popular choice across all categories of age and voting history, and that nonvoters – those who had not participated in any previous elections since 1998 – were the most likely to vote in person on election day.

Two of the variables of interest, race and education, are not significant in the second model. In the first model, education is significant for the decision to vote in person versus not voting, but it is not significant for the choice to vote by Internet versus not voting. Race is only significant in the first model for the decision to vote in person versus not voting, but the effect is small. Both variables reach significance when they are interacted with voting history, which suggests that it is the combination of voting history and these demographic variables that has an effect on voting choice, but even here the effect is small. An infrequent voter living in a zip code that is 80% black has a 34% likelihood of voting on the Internet and a 13% likelihood of voting by mail, compared to an infrequent voter living in a zip code that is 20% black who is just one percentage point more likely to vote on the Internet and has the same likelihood of voting by mail.

6 Conclusion

This research shows that Internet voting as an early voting reform helps bring two groups into the electorate who might not otherwise have voted: young people and people who were infrequent voters. These findings are important for policy makers and election administrators to consider when evaluating new voting reforms, since they provide evidence that Internet voting can be effective at bringing young voters into the electorate. They are also important in light of the recent research on voting reforms, which have been almost unanimous in their findings that no new groups of voters are drawn into the electorate.

Since voting history has been shown to be an important predictor of future voting behavior, new studies of the effects of voting reforms on individual voters must include information about voting history. State voter registration files should be utilized by political scientists, as they are used by political professionals, to inform predictions and explanations about voting behavior and the effects of early voting reforms. The Help America Vote Act of 2002 has helped states streamline their voter registration databases, and these advances should aid political scientists in obtaining state voting archives that are suitable for research purposes.

Several state legislatures have proposed an expansion of no-excuse absentee mail programs, and some states are even considering adoption of all vote-by-mail systems like Oregon's. According to electiononline.org, a non-partisan election reform advocacy organization, there is legislation currently pending in 19 states to expand mail absentee voting programs. This research suggests that states should also consider implementing Internet voting as an absentee voting method, if the goal of reformers is to encourage voting among young people. This research also suggests that a switch to all mail voting programs could actually decrease turnout among young voters.

Of course there are many concerns about Internet voting that are not addressed in this paper, including security concerns that some scholars suggest are insurmountable in large-turnout public elections [Ca00]. However, I believe the implications for young voters are so important that more experiments with Internet voting as an early voting method should be tried. Alvarez and Hall agree that more controlled experiments with Internet voting should be designed and implemented in order to learn more about the effects on turnout among demographic groups and the potential security risks [AH04]. As an early voting method, Internet voting can be implemented in a way that is very similar to a traditional absentee ballot, as it was in the 2004 Michigan primary. The important distinction for young voters is that instead of going to a post office, voters go to a website to vote, and in this election that seems to have made a difference.

Appendix

Dependent Variable

Participation in the 2004 Michigan 4 categories, coded:

Democratic Presidential Primary 0 = Did not vote

1 = Voted in person

2 = Voted by Internet

3 = Voted by Mail

Explanatory Variables

Age Voter's age in years, taken from the birth year listed on the Michigan Qualified Voter File.

Gender Coded 0 for Male and 1 for Female, taken from the Michigan Voter File.

Income Median income in the voter's zip code of residence, in thousands, taken from the 2000 Census.

Education Percent college educated in the voter's zip code of residence, taken from the 2000 Census.

Race Percent African American in the voter's zip code of residence, taken from the 2000 Census.

Zip Code Voter's zip code of residence.

2000 Gore vote: Percent of the vote for Al Gore in 2000 by State House district, adjusted for the 2002 state legislative redistricting, provided by Brian F. Schaffner of American University.

Vote History Variables

Vote history data is from the Michigan Qualified Voter File and includes information for the following elections: 1998 primary and general, 2000 primary and general, 2002 primary and general.

Nonvoter: Coded 1 for individuals who did not participate in any of the elections taken from the state voter file; coded 0 otherwise.

Infrequent voter Coded 1 for individuals who participated in at least 1 general election but no primaries; coded 0 otherwise.

Occasional voter Coded 1 for individuals who participated in at least 1 primary election; coded 0 otherwise.

Regular voter Coded 1 for individuals who participated in all of the last 3 elections (the 2002 general and primary and the 2000 general); coded 0 otherwise.

References

[AH04] Alvarez, R. M.; Hall, T.: Point, Click, and Vote: The Future of Internet Voting. Washington, DC: Brookings Institution Press, 2004.

[AN01] Alvarez, R. M.; Nagler, J.: The Likely Consequences of Internet Voting for Political Representation. Loyola Law Review, 34, 2001; pp.1115-1153.

[Be05] Berinsky, A.: The Perverse Consequences of Electoral Reform in the United States. American Politics Research 33, 2005; pp. 471-491.

[BBT01] Berinsky, A.; Burns, N.; Traugott, M.: Who Votes By Mail? A Dynamic Model of the Individual Level Consequences of Voting-By-Mail Systems. Public Opinion Quarterly 65, 2001; pp.178-197.

[Ca00] California Internet Voting Task Force Report: 2000. Retrieved on May 1, 2008, from http://www.sos.ca.gov/executive/ivote/

[DK00] Darden, J.; Kamel, S.: Black Residential Segregation in the City and Suburbs of Detroit: Does Socioeconomic Status Matter? Journal of Urban Affairs 22, 2000; pp. 1-13.

[GGS03] Gerber, A.; Green, D.; Shachar, R.: Voting May Be Habit-Forming: Evidence from a Randomized Field Experiment. American Journal of Political Science 47, 2003; pp. 540-550.

[GBN96] Geronimus, A.; Bound, J.; Neidert, L.: On the Validity of Using Census Geocode Characteristics to Proxy Individual Socioeconomic Characteristics. Journal of the American Statistical Association 91, 1996; pp. 529-537.

[Gi02] Gibson, R.: Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary. Political Science Quarterly 116, 2002; pp. 561-583.

[Gr04] Gronke, P.: Early Voting Reforms and American Elections. Paper presented at the 2004 Annual Meeting of the American Political Science Association.

[NR01] Neeley, G.; Richardson, L.: Who is Early Voting? An Individual Level Examination. The Social Science Journal 38, 2001; pp. 381-392.

[Ol96] Oliver, E.: The Effects of Eligibility Restrictions and Party Activity on Absentee Voting and Overall Turnout." American Journal of Political Science, 40, 1996; pp. 498-513.

[Pl02] Plutzer, E.: Becoming a Habitual Voter: Inertia, Re-sources, and Growth in Young Adulthood. American Political Science Review 96, 2002; pp. 41-56.

[PS08] Prevost, A.; Schaffner, B.: Digital Divide or Just Another Absentee Ballot? Evaluating Internet Voting in the 2004 Michigan Democratic Primary." American Politics Review, forthcoming, 2008.

[RH93] Rosenstone, S.; Hansen, J.: Mobilization, Participation, and Democracy in America. New York: MacMillan Publishing Company, 1993.

[So04] Solop, F.: Digital Democracy Comes of Age: Internet Voting and the 2000 Arizona Democratic Primary Election. PS: Political Science and Politics 34, 2001; pp. 289-293.

[SG97] Stein, R.; Garcia-Monet. P.: Voting Early but Not Often. Social Science Quarterly 78, 1997; pp. 657-671.

[TK79] Traugott, M; Katosh, J.: Response Validity in Surveys of Voting Behavior. Public Opinion Quarterly 43, 1979; pp. 359-377

[Tr04] Traugott, M.: Why Electoral Reform Has Failed: If You Build It, Will They Come?" In (A.N. Crigler, M. R. Just, and E. McCaffery): Rethinking the Vote: The Politics and Prospects of American Election Reform. New York" Oxford University Press.

Session 3: Legal & Procedural Issues of E-Voting

A Methodology for Assessing Procedural Security: A Case Study in E-Voting

Komminist Weldemariam[1,2], Adolfo Villafiorita[1]

[1]Fondazione Bruno Kessler
Center for Scientific and Technological Research (fbk-irst)
Sommarive 18 I-38050 Povo (TN) – Italy
{sisai|adolfo}@fbk.eu

[2]DISI, University of Trento
Sommarive 14 I-38100 Povo (TN) – Italy
weldemar@disi.unitn.it

Abstract: This paper presents a methodology for procedural security analysis in order to analyze and eventually try to make elections more secure. Our approach is based on modelling the electoral procedures in the form of business process models (which we write in a strict simplified subset of UML), systematically translate the models into executable formal specifications, and analyze the specifications against security properties. We believe such an analysis to be essential to identifying the limits of the current procedures (i.e. undetected attacks) and to identify more precisely under what hypotheses we can guarantee secure elections. This paper presents the approach and demonstrates with an example taken from the e-Voting procedures enacted within the ProVotE project, current trial of the Italian legislation.

1 Introduction

The organization of elections in Italy involves various offices of the Public Administration and private contractors, has a time-span of months, and has strict security and traceability requirements. Sensibility by citizens and politicians is very high, and litigation over, e.g., implementation of procedures and validity of results are not uncommon. The Autonomous Province of Trento who has autonomy over local election is evaluating the switch to e-voting and, to that extent, is sponsoring the ProVotE project [VF06].

The switch to electronic elections in Italy, however, is a long and difficult process that requires extreme attention, including a thorough understanding of the limits of the risks associated to the procedures or to the combination of the procedures and systems chosen for voting. (See, e.g., [ALRL04; Mya05; FM06; MFMP07; BLRS06; LKK+03; Ale04] for a discussion of security risks associated to the usage of ICT systems and elections.)

We are approaching the problem by reasoning about the procedures and controls that regulate the usage of e-voting systems. We do so by providing formal models of the procedures, by "injecting" threats in such models and by analyzing, through the help of model checker, the effects of such threats. We believe such an analysis to be essential to, first, identifying the security boundaries— that is the conditions under which procedures can be carried out securely and, secondly, devise a set of requirements, to be applied both at the organizational level and on the (software) systems used to make systems and system processes secure. In particular, the violation of security properties could provide clues about a sequence of actions that an adversary uses to construct attacks before or during the execution of procedures.

The main contribution of this paper is twofold. On one hand we are tackling the problem at the procedural level —namely, we are trying to understand weaknesses and strengths of the procedures regulating an election, in order to analyze possible attacks and their effects on the electoral system, and, more specifically, possible attacks and threats that can be realistically carried out on the e-voting machines. On the other hand, we are interested in devising techniques and tools to analyze security threats at the organizational/procedural level, and eventually make comparison between as-is and to-be election system procedures.

This paper refines and extends the work presented in [WVM07], and it is structured as follows. In the next chapter we explain the ProVotE project scopes under which this work has been developed. In Chapter 3, we describe the context of procedural security in detail. In Chapter 4, we describe our methodology for procedural security analysis and illustrate the approach with an example in Chapter 5. Finally, in Chapter 6, conclusions drawn from this work are discussed.

2 The ProVotE Project and Motivations

ProVotE [VF06], a project sponsored by Provincia Autonoma di Trento (PAT), has the goal of ensuring a smooth transition to e-voting in Trentino, eliminating risks of digital divide and providing technological solutions which support, with legal value, the phases ranging from voting to the publication of the elected candidates.

The project includes partners from the public administration (PAT, Regione Trentino/Alto-Adige, Consorzio dei Comuni Trentini, Comune di Trento, IPRASE), research centers and academia (FBK, Faculty of Sociology of the University of Trento, Fondazione Graphitech), and local industries (Informatica Trentina). The technological solution (both software and some hardware components) has been developed in house, providing integration with some commercial components.

The project is multi-phased and is organized in various lines of activities that strictly interact (see also [VF06; CBF+06] for more details).

The first phase had the goal of testing prototypes, evaluating acceptance by citizens, ease of use, and some organizational aspects. Verification of the results achieved in the first phase was conducted through four different trials (between 2005 and 2006) held during local elections. Participation to the first phase has been quite high: about 10,000 citizens took part in the experimentation[30].

During the second phase of the project we used the electronic systems in two elections, with legal value. The first election was the election of student representatives in a local high school and it involved 1,298 students. The second election — conducted in the towns of Campolongo al Torre and Tapogliano in Friuli-Venezia Giulia (November 2007), a neighboring region with autonomy similar to that of PAT — was a poll to unify the two municipalities; 561 people used the system.

For the third phase of the project, which could lead to a large-scale introduction of the new voting system, aspects related to procedures, logistics, and organization become more relevant, as they will serve both as the basis for the deployment of the solution and for the definition of the laws that will govern the electronic election.

With respect to scope, population, and participation, ProVotE is among the largest, if not the largest, e-voting project in Italy.

3 The Context of Procedural Security Analysis

Procedural security deals with the identification, modelling, establishment, and enforcement of security policies about the procedures that regulate the usage of a system and system processes.

The situation is depicted in Figure 1. *Our target of evaluation* is a complex organization setting in which procedures transform and elaborate *assets,* which may not necessarily be just digital assets (like, e.g., paper documents are also sensitive assets). The procedures and the organization are meant to add value to the assets and high desire to protect them from attacks, which can either come from external sources or from insiders.

[30] Detailed results of all the experimentations and elections conducted within the ProVotE project are available on the Internet at: http://www.provincia.tn.it/elezioni and http://referendum2007.regione.fvg.it/index.html.

In particular, we distinguish the following kind of attacks:

1. *Attacks on digital assets* (item 1 and item 3 in Figure 1). These attacks are meant to alter one or more of the digital assets of an organization. Attacks can either be carried out from external sources (the environment) or from internal sources. Opportunities for attacks are determined by the organizational setting and by the security provided by the digital systems.

2. *Attacks on other kinds of assets* (item 2 and item 4 in Figure 1). These attacks are meant to alter one or more of the non-digital assets of an organization. Attacks can either be carried out from external sources (the environment) or from internal sources. Opportunities for attacks are determined by the organizational settings only.

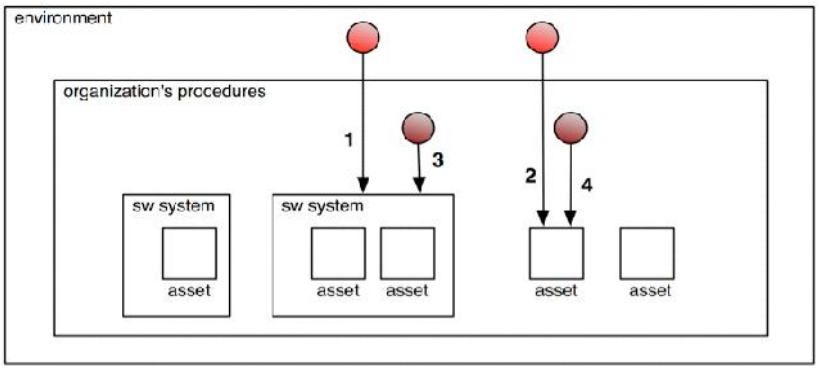


Figure 1: Procedural security Analysis.

Security assessment usually focuses on understanding items 1 and 3, namely, types and effects of attacks on (software) systems. In order to address the scenario depicted above in a systematic and tool-supported way, we *lift* the security assessment at the organizational level and we call *procedural security* analysis the usage of techniques and tools to understand the impact and effects of *procedural threats*, namely courses of actions that can take place during the execution of the procedures and which are meant to alter the assets manipulated by procedures in an unlawful way.

4 A Methodology for Procedural Security Analysis

We developed a precise methodology to perform formal procedural security analysis, based on the following steps (see also Figure 2):

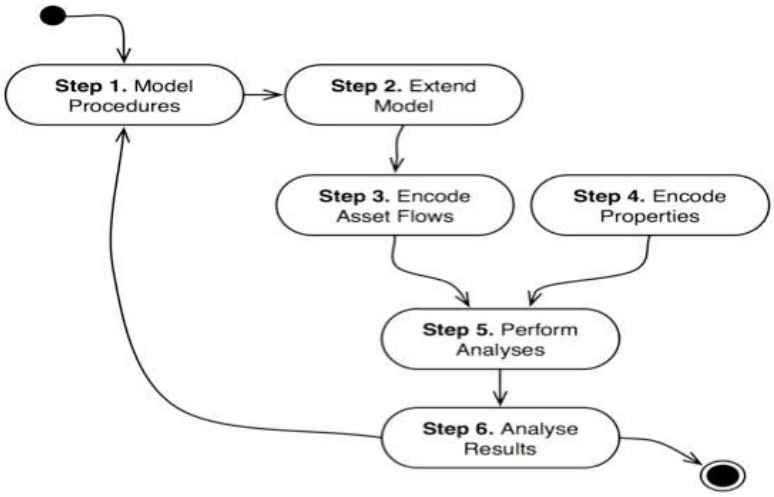


Figure 2: The process of formal procedural security.

1. ***Provide (business) models of the procedures under evaluation***. The starting point is a model that describes the process or the processes to be analyzed (Step 1 of Figure 2). In order to ease the task of translating the models into executable asset-flows, we defined and stuck to a subset of the UML activity diagrams. This allows us to describe the concepts like asset, processes, and accessory information (such as, location) in a strict and defined way. So far we managed to provide UML models of the electoral procedures in place in the Autonomous Province of Trento and in Regione Friuli Venezia Giulia. We use Visual Paradigm[31] as our reference-modelling tool. See some previous works [Man03; Mat06; Cia07] for more details about the notation, tool support, and the model themselves.

[31] http://www.visual-paradigm.com/

2. ***Inject Threat actions into the model***. We generate, from the models defined at the previous step, what we call *extended model* (Step 2 of Figure 2). The extended model is generated by "injecting" asset-threats in the nominal flow of the procedures. Thus, in the extended model, not only assets are modified according to what the procedures define, but they can also be transformed by the (random) execution of one or more threat actions. The possible impact of threats depends upon the injection strategy that is chosen. The most general strategy is that of injecting all possible threats at all possible steps of the process (the model checker will take care of "pruning" useless threats, namely threats which do not lead to any successful attack). The construction of the extended model, whose generation can be automated, is currently performed by hand.

3. ***Encode the Asset Flows***. From the extended models defined at the previous step we derive the asset flows of each asset manipulated by the procedures (Step 3 of Figure 2). Asset flows are represented in the NuSMV input language. The NuSMV model of the asset flows is based on the definition of "program counters" that ensure that procedures are executed according to the specifications, and by defining one module per asset with one state variable per asset-feature. The state variables encode how features change during the execution of the procedures. Accessory information, such as actors responsible for the different activities, can be used, e.g., to enrich the language used to express security properties. The necessity of modelling actors' roles in NuSMV depends upon the target of the security analysis. Note that from the list of activities executed to carry out, e.g., an attack, we can derive the list of actors involved, simply by looking at the UML activity diagrams.

4. ***Specify Security*** Properties to Check. The specifications of the desired (procedural) security properties, namely, the security goals that have to be satisfied, are then encoded using LTL/CTL formulas (Step 4 of Figure 2), which then (together with the model) are given as input to NuSMV.

5. ***Perform Analysis***. We finally run the model checker to perform the analyses (Step 5 of Figure 2). Counterexamples of security properties encode the sequence of actions that have to be executed in order to carry out an attack on an asset.

6. ***Analyze Results***. The last step is analyzing the obtained results (Step 6 of Figure 2). Counterexamples are used to achieve the following two goals. First, they allow to understand what are the hypotheses and conditions under which a given security goal is achieved or breached. Second, they provide information to try and modify the existing procedures, so that security breaches are taken care of. Analogously to what happens in safety analysis when analyzing, e.g., the loss of critical functions, enhancing the procedures results in reducing the probability of an attack or making the attack more complex, rather than eliminating it [Mar07].

5 A Case Study Example

Modelling Asset-flow, Step 1. Figure 3 shows a fragment of the procedure that is followed during project trials for the transfer of election results from polling stations to Electoral Office. The diagram abstracts away those details that are irrelevant for the sake of presentation, e.g. details related to the alternative modelling choices for carrying out the data transfer process are omitted. We also hide some actors' responsibilities by collapsing, e.g. Secretary, Scrutinizers, them into a single actor. See in [Vol07] for detail strategies of data transfer process and how the alternative choices are modelled.

The diagram illustrates (see Figure 3), after the election, the Section President (one of the Poll Officers) deactivates the voting machines, extracts (from the voting machine) printed votes, the USB key with the results, and other artifacts, and prepares a package containing votes and various reports, to be delivered to the Electoral Office. Electronic data are transmitted through a VPN and the USB key with the electronic results delivered to the Electoral office via a "messenger" (e.g. a police officer).

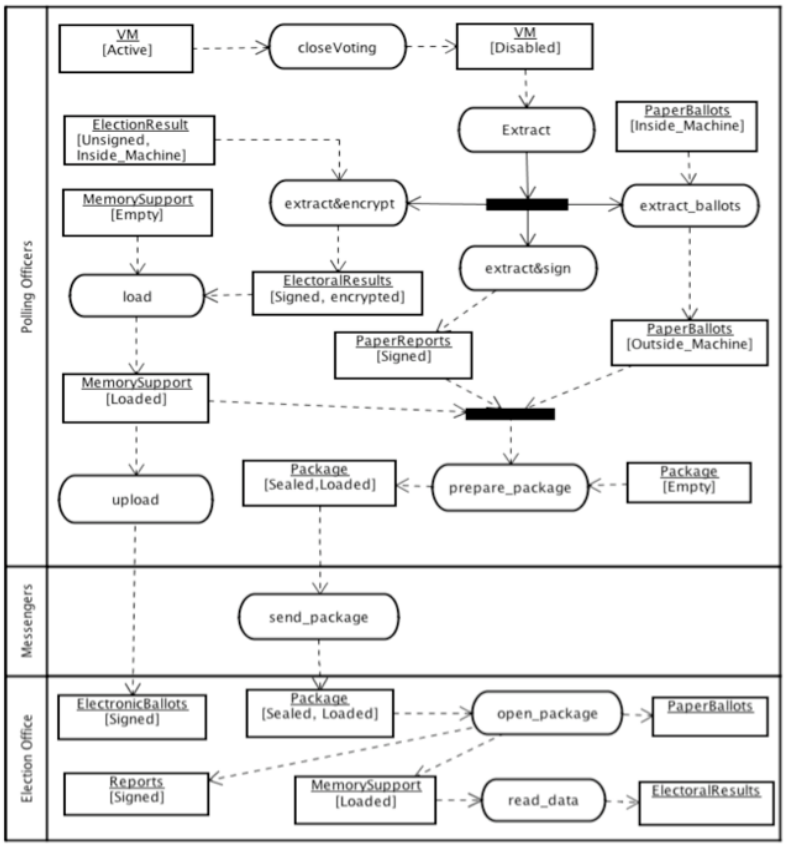


Figure 3: An example of asset flow.

Threat Injection, Step 2. The next step is *injecting*, that is, extending the model with threat actions and generate the *extended model*. Figure 4 shows some examples of threat-actions injected into the nominal model of Figure 3. In the extended model, threat actions are marked with the stereotype "threat-action". Impact of the attacks depend upon the asset they target and the position, in the procedure, where the attack take place.

For instance, replacing the results of a polling station in a USB key has no effect after the result have been generated. (On the other hand it may change the results of the election if performed before the results have been computed.)

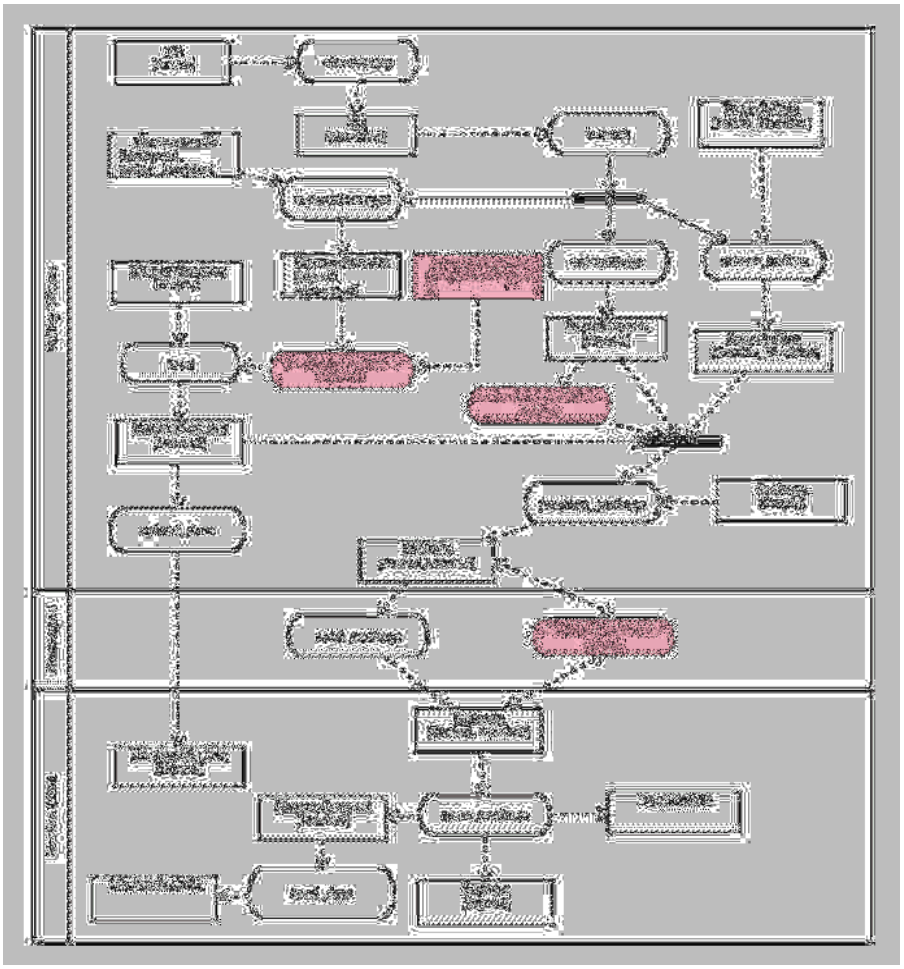


Figure 4: An example of extended model.

Asset-Flow encoding, Step 3. Below we show a snippet of the code that defines the asset type *electionResult* and some of its feature variables, named *state* (the states in which the *electionResult* can be) and the content (the qualitative value of the *electionResult* can be).

```
MODULE electionResult ( ... )
VAR
state     : {plain,unsigned,signed,signed_&_encrypted};
content : {null,data,signed_&_encrypted_data,garbage};
```

The evolution of assets' properties is encoded using state machines, which are encoded in NuSMV with the *next* construct (which specifies the value of a variable at step *n+1,* given the value at step n). Below, for instance, we show a piece of NuSMV code that illustrated how the content variable of *electionResult* asset changes:

```
init(content) := null;
next(content) := case
pc.pc = closeVoting && next(pc.pc) = extract_&_encrypt : data;
content = data && pc.pc = extract_&_encrypt && state = signed: signed_&_encrypted_data;
[...]
```

Threat injection (model extension) corresponds to augmenting the state machine of the asset flow with new transitions (e.g., adding a transition that leads to a *garbage* state of *content*) corresponding to the execution of threat actions. The triggering of a threat action is "monitored" through boolean variables that are set to true when the action takes place, as illustrate by the following pieces of code:

```
next(can_malElectionRes) := case
  (malElectionRes && pc.mpc = replaceElectionRes &&
  next(electionResult.content) = malEnSignedData) || [...]  :1;
  1: can_malElectionRes;
  esac;
```

Note that in the codes above we have left some detail specification (such as location) for the matter of presentation purposes. Analogously, the remaining asset flows and model extension encodings can be encoded.

Specify Security Properties and Perform Analysis, Step 4 & 5. We use temporal logic formulas to represent the properties of interest and model check them using the NuSMV tool. In particular, security properties are specified using LTL/CTL logic language. LTL is used to reason on the computational path scenarios of an asset (e.g., what can happen as asset travels along different locations), while CTL to reason about the existence of specific states (e.g., is there any particular state in which an asset can be altered in an undesired way).

Among the property classes we are interested in is that of verifying a property about "*Safe transfer of election result.*" A desirable property, for instance, that we want to specify and analyze can be described in plain text as: "*It is never the case that election officials receive modified election data before computing the final result.*" This property is expressed in CTL formula as:

AG ! (ElectionResult.can_garbage && ElectionResult.location = electoralOffice)

We give the above property to NuSMV tool to check that the property holds. However, the tool generates a counter-example showing the violation of the given property. Upon analyzing the generated counter-example, the election result is replaced (i.e., a replace attack is in place) following the introduction of a wrong election data into the asset flow, which, in turn, causes wrong delivery of election result to the electoral office. Among the possible scenarios that we analyzed, at some time a malicious election data is introduced while poll officer is preparing the data to transfer to electoral office. At the same time, an attacker implements replace attack before loading the memory support.

6 Related Work

Various approaches (for specifying, modelling, analyzing, and assessing security) have been proposed in the past and proven useful for zeroing the security lacks of the analyzed systems (see, for instance, [FM06; BDL+03; VWW06; Wim05]).

To our knowledge, however, formal procedural security analysis is quite an un-explored area. The work closest in spirit to ours can be found in [XM04, XM05], where the authors argue the need for procedural security in electronic elections and provide various examples of procedural risks occurred during trials in the UK; in [LKK+03, XM06] where the authors highlight the importance of defining roles and responsibilities in e-voting and in [Ale05] where the need for applying business process re-engineering to the electoral process is emphasized. Our focus, however, is on the technical machinery to automate analyses.

Volha et al. [Vol07] presents an approach to reason on security properties of the to-be models (which are derived from *as-is* model) in order to evaluate procedural alternatives in e-voting systems using Tropos.

Finally, Alexander et al. in [PKKU04] also highlighted a comprehensive way of overviewing attacks against sensible assets in all stages of e-voting.

7 Conclusion

In this paper we presented a methodology to perform procedural security analysis based on explicit reasoning on asset-flows — notably, by building a model to describe the nominal procedures implementation, enriching this model with possible threat actions, and encoding the extended model to suit for model checking techniques which, in turn, allows to reason on different aspects of the procedures such as, the "actor-play-role" principle and some reachability analysis for some undesired state of an asset. Among the advantages of our approach, the possibility of getting a better comprehension of the effect and impact of combined attacks to the assets of an election.

The model checker runs that were made on the current version of the specification have not revealed much interesting results though seemed useful; therefore, much work needs to be done in order to see if the model can be fully verified or if any interesting results can be uncovered. Moreover, we need to consolidate our approach and provide guidelines that can be incorporated in the Common Criteria [cc07], both methodologically and in a tool supported way to automate the analysis.

References

[Ale04] Alexandros Xenakis and Ann Macintosh. Levels of Difficulty in Introducing e-Voting. Electronic Government, 3183/2004, November 05 2004. LNCS, Springer.

[Ale05] Alexandros Xenakis and Ann Macintosh. Using Business Process Re-engineering (BPR) for the Effective Administration of Electronic Voting. The Electronic Journal of e-Government, 3(2), 2005.

[ALRL04] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, 01(1):11–33, 2004.

[BCP+02] P. Bertoli, A. Cimatti, M. Pistore, M. Roveri, and P. Traverso. NuSMV 2: An Open Source Tool for Symbolic Model Checking. In Proceeding of International Conference on Computer-Aided Verification, 2002.

[BDL+03] David Basin, Jürgen Doser, and Torsten Lodderstedt. Model Driven Security for Process-Oriented Systems. In SACMAT ’03: Proceedings of the eighth ACM symposium on Access control models and technologies, pages 100–109, New York, NY, USA, 2003. ACM.

[BLRS06] J W. Bryans, B Littlewood, P Y. A. Ryan, and L Strigini. E-Voting: Dependability Requirements and Design for Dependability. ARES ’06: Proceedings of the First International Conference on Availability, Reliability and Security (ARES’06), 0:988–995, 2006.

[CBF+06] Letizia Caporusso, Carlo Buzzi, Giolo Fele, Pierangelo Peri, and Francesca Sartori. Transition to Electronic Voting and Citizen Participation. In Robert Krimmer, editor, Electronic Voting, volume 86 of LNI, pages 191–200. GI, 2006.

[cc07] Common Criteria. 2007. http://www.commoncriteriaportal.org/.

[Cia07] Aaron Ciaghi. From Laws to Models: Tools and Methodologies. Master’s thesis, University of Trento, Italy, 2006-2007. In Italian.

[FM06] Igor Nai Fovino and Marcelo Masera. Through the Description of Attacks: A Multidimensional View. In Computer Safety, Reliability, and Security, 25th International Conference, SAFECOMP 2006, Gdansk, Poland, September 27-29, 2006, Proceedings, pages 15–28, 2006.

[LKK+03] Costas Lambrinoudakis, Spyros Kokolakis, Maria Karyda, Vasilis Tsoumas, Dimitris Gritzalis, and Sokratis Katsikas. Electronic Voting Systems: Security Implications of the Administrative Workflow. In DEXA '03: Proceedings of the 14th International Workshop on Database and Expert Systems Applications, page 467, Washington, DC, USA, 2003. IEEE Computer Society.

[Man03] Andrea Mattioli. From Processes to Information Systems: Tools for Sharing Models. Master's thesis, University of Trento, Italy, 2002-2003. (In Italian)

[Mar07] Marco Bozzano and Adolfo Villafiorita. The FSAP/NuSMV-SASafetyAnalysisPlatform. Int. J. Software Tools Technology Transfer, 9(1):5–24, 2007.

[Mat06] Andrea Mattioli. Analysis of Processes in the Context of Electronic Election. Master's thesis, University of Trento, Italy, 2005-2006. (In Italian)

[MFMP07] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems. Comput. Stand. Interfaces, 29(2):244–253, 2007.

[Mya05] Myagmar, S. and Lee, A. and Yurcik, W. Threat Modelling as a Basis for Security Requirements. In StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability, pages 94–102,, New York, NY, USA, 2005. ACM Press.

[PKKU04] Alexander Prosser, Robert Kofler, Robert Krimmer, and Martin Karl Unger. Security Assets in E-Voting. In Electronic Voting in Europe, pages 171–180, 2004.

[VF06] Adolfo Villafiorita and Giorgia Fasanelli. Transitioning to e-Voting: the ProVotE Project and the Trentino's Experience. In EGOV-06, Krakow, Poland, 2006.

[Vol07] Volha Bryl, Fabiano Dalpiaz, Roberta Ferrario, Andrea Mattioli and Adolfo Villafiorita. Evaluating Procedural Alternatives. A Case Study in e-Voting. Proceedings of MET-TEG07, 2007. An extended version has been published as a Technical Report DIT-07- 005, Informatica e Telecomunicazioni, University of Trento.

[VWW06] Monika Vetterling, Guido Wimmel, and Alexander Wisspeintner. A Graphical Approach to Risk Identification, Motivated by Empirical Investigations. Lecture Notes in Computer Science, pages 574–588, Thursday, November 23 2006.

[Wim05] Guido Oliver Wimmel. Model-Based Development of Security-Critical Systems. PhD thesis, German umlauts Institut f¨r Informatik der Technischen Universität München, February 2005.

[WVM07] Komminist Weldemariam, Adolfo Villafiorita, and Andrea Mattioli. Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach. In Ammar Alkassar and Melanie Volkamer, editors, VOTE-ID, volume 4896 of Lecture Notes in Computer Science, pages 38–49. Springer, 2007.

[XM04] Alexandros Xenakis and Ann Macintosh. Procedural Security Analysis of Electronic Voting. In ICEC '04: Proceedings of the 6th international conference on Electronic commerce, pages 541–546, New York, NY, USA, 2004. ACM Press.

[XM05] Alexandros Xenakis and Ann Macintosh. Procedural Security and Social Acceptance in E-Voting. In HICSS '05: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 5, page 118.1, Wash- ington, DC, USA, 2005. IEEE Computer Society.

[XM06] Alexandros Xenakis and Ann Macintosh. A Generic Re-engineering Methodology for the Organized Redesign of the Electoral Process to an E-electoral Process. In Electronic Voting, pages 119–130, 2006.

Secure Remote Voter Registration

Victor Morales-Rocha[1], Jordi Puiggalí[1], Miguel Soriano[2]

[1]Scytl Secure Electronic Voting
Tuset 20 1-7 Barcelona, Spain
{victor.morales| jordi.puiggali}@scytl.com

[2]Technical University of Catalonia
Department of Telematics Engineering
Jordi Girona 1-3 Barcelona, Spain
soriano@entel.upc.edu

Abstract: Voter registration is an important issue in election processes. In order to protect the election accuracy, it is necessary to have an accurate electoral roll of eligible voters. The electoral roll is usually constructed by means of a voter registration system that compiles voter data either in person or remotely. Current solutions for remote voter registration lack effective methods to prevent impersonation, multiple registrations and alterations on voter information. In this paper we propose a remote voter registration scheme that increases the accuracy of the current systems. In this scheme the voter identification is carried out by means of some biometric systems. Biometrics is also used to prevent impersonation, detect multiple registrations from the same person and protect from alterations of the registration information.

1 Introduction

Lately, there has been an increasing interest to improve the efficiency in the election processes, which has resulted in a wide range of proposals for new election systems. Most of the proposals have been focused in voting and tallying stages, giving least interest to voter registration stage.

Voter registration is the process of collecting the voters' data in order to constitute an electoral roll. Because of the fact that the electoral roll determines if a voter has the right to cast a vote during the voting stage, it has to be formed in an efficient way. Even when voting and tallying stages have the greatest security level, a deficient voter registration system can facilitate fraud practices that can even affect the accuracy of the election.

Voter registration is conventionally carried out face to face with the registration authority. However, since many voters are residing abroad during an election process, it has been necessary to have new methods to collect, remotely and in a secure manner, the information of such voters. As in most of the remote transactions, current remote voter registration systems face some security problems. These problems are mainly related to the inability to accurately verify the identity of the voter, which can facilitate impersonation or multiple registrations by the same voter with different data [El07].

In this paper we propose a remote voter registration scheme, in which some biometric systems play an important roll to protect the accuracy of the electoral roll. Biometric systems have already considered in electronic voting in the voting phase, e.g. [Ho07]. However, they have not been extensively used in the voting or in the registration phase.

It is important to note that sometimes voter registration is related to the voter credential generation process. Some authors have made proposals about this subject [Ac04, Kr07, Sc06]. However, in the context of this paper, voter registration is related to the creation of the electoral roll.

Section 2 presents a panorama of the current voter registration systems, as well as an analysis of biometrics and how these can be applied to improve the voter registration process. In section 3, our proposal is described. Section 4 concludes by emphasizing the advantages that our proposal gives to the remote voter registration process.

2 Voter Registration

2.1 Current Voter Registration Systems

Nowadays, in some countries like The United States [Fv08] or United Kingdom [El08] it is common to carry out remote voter registration. These methods allow the voter to fill out his or her own paper registration form remotely (e.g., at home) and return this form to the registration officers by using a delivery channel or optionally attending in person to a registration site. Registration forms are usually available to voters through postal delivery or downloading them from the network. In both cases voters fill out handwrite sign and return the forms to the registration officers using a postal delivery or any other alternative channels such as fax or e-mail (attaching a scanned copy of the filled form) [Fv08]. Furthermore, there are countries [De06] introducing the use of web interfaces to allow voters to fill out the registration form online, speeding up the remote acquisition of voter registration information.

After sending the registration form, if a voter wishes to verify that the registration has been received by the registration officers, he or she can contact them through e-mail or a phone call.

In the cases previously described, the identification of the voter is done by one or the combination of the following techniques: the verification of personal information of the voter and the verification of some physical characteristics of the voter. The first technique consists of registration officers checking to see if the voter included in the form some personal information that it is also stored in the voter register. Some examples could be the date of birth, the social security number or any other familiar information (e.g., mothers' maiden name, etc.). The problem with using such information for identifying the voter is that this information could be available in other databases (e.g., the member database of a social club) or could be known by people close to the voter. Therefore, it could be easy to impersonate a voter in the registration process just using this information.

The second technique consists of requiring verifying the identity of the voter based on checking some voter personal characteristics, such as a handwriting signature stamped on the form or the face or fingerprint of the voter against an image or template contained in some identity card or database. Face recognition requires the physical presence of the voter and therefore, it is not suitable for a real remote voter registration. However, handwriting recognition is the usual way implemented by remote registration and therefore the main one considered in this paper. In any case, the accuracy of this second technique of voter identification is based on the ability of the registration officers to validate the voter authentication data. Considering that most of these officers are not handwriting or physiognomy experts, we cannot expect high levels of accuracy.

Furthermore, current remote voter registration methods do not check if the same person has filled out more than a registration form by using the names of different valid voters. That is, using handwriting signatures as a reference, the verification process is based on looking for similarities between the signature on the form and a pre-existing signature. Therefore, detecting a person filling out more than one registration form signed with different signatures could be unfeasible for a registration officer. In this case, registration officers must have the ability to extract the identity of a person from the handwriting signature instead of looking for similarities. It is important to mention that registration officers usually do not have a pre-existing signature of the voter. Therefore, the signature contained in the registration form is only used to create a temporary database of signatures that will be used to identify the voters during the vote casting process. For example, in the case of postal voting, the voter signature stored during the registration process is compared against the signature contained in the postal envelope to detect if the vote has been cast by the legitimate voter.

Finally, in addition to identification accuracy, there are additional problems in current remote registration scheme. The contents of the registration form can be altered after the voter has sent this form. Furthermore, the handwriting signature on the form can be re-used by an attacker to fill out a different registration form. This problem lies in the fact that handwriting signatures (as well as face recognition) are not bound to the contents of the register. Therefore, any change in the contents of the registration form or the re-use of a valid handwriting signature in a different form cannot be detected by simply verifying the signature.

Summarizing, current voter registration systems face the following problems:

- Accuracy to validate the voter identity;
- Prevention of multiple registers by voters; and
- Integrity of voter registration information.

To increase the accuracy of remote registration process, we propose the combination of biometric systems and cryptographic functions. Below we analyze which are the improvements of adding both techniques in remote registration process.

2.2 Accuracy on Biometric Systems

In some way, the voter registration systems previously described are based on the use of biometrics. Registration officers usually verify some physical characteristics that uniquely identify the voter, such as a picture (facial identification) or the signature of the voter. However, one of the main issues of this identification is the accuracy on the process, since not all the registration officers are, for example, handwriting or physiological experts. In this sense, we propose the use of biometric systems to help registration officers to improve the accuracy of voter identification. However, are all the biometrics systems suitable for a remote voter registration?

Biometric systems are electronic systems specialized on identifying a user by means of processing unique physiological or behavioural characteristic of the user. Biometrics systems are classified based on the unique characteristic of the user that is used for the identification, for instance: DNA, face, fingerprint, iris, palmprint, retina, writing/signature and voice. However, the accuracy on the different biometric system is not the same, since each of the biometric characteristics processed has advantages and disadvantages.

A good biometric characteristic must fulfil some requirements [JR04]:

- Universality- Each individual should have the characteristic.
- Uniqueness- How well the characteristic makes different two individuals.
- Permanence- How well the characteristic endures over time.
- Collectability- Ease of acquiring the characteristic.
- Performance- Refers to the speed and accuracy of recognition as well as the resources required to do it (cost).
- Acceptability. It indicates the level of acceptance of people to use the characteristic.
- Robustness. It reflects the level of resistance against fraudulent methods attempting to mislead the system.

In our analysis, we considered an additional requirement for remote voter registration: the biometric system must be remotely available for most of the voters. Therefore, the acquisition of the biometric information must be supported using standard means or devices. This reduces the number of potential candidates to handwriting signatures and voice biometrics, since these allow biometric information to be acquired by means of scanning the signature written in the paper registration form or a voice recording made from a standard telephone. About handwriting biometrics, there are two distinct techniques, namely on-line and off-line handwriting. Besides the shape of the signature, on-line signatures take into account other aspects such as pen timing, pressure or writing trajectory. However, we do not consider on-line signatures a good candidate, since it requires voters to have available a digital-pad for acquiring a writing of a text (e.g., the signature of the voter). Therefore we will focus on off-line signatures.

Using pre-existing biometric systems comparative analysis [JR04, Ti06] and taking fingerprint biometrics as reference, the proposed biometrics systems fulfil the requirements previously introduced as follows (L=Low, M=Medium and H=High).

Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Robustness**
Fingerprint	H	H	H	M	H	M	M
Off-line Signature	M	M	L	H	L	H	L
Voice	M	M	M	H	M	H	L

Table 1. Comparison of three example biometric systems

From this comparison we can conclude that off-line signatures and voice biometrics are not as robust as fingerprint biometrics systems. However, the introduction of voice biometrics could improve the current systems based on handwriting signatures.

Another important aspect of performance on biometrics is the accuracy of the identification process. There are three parameters that can help to determine in a quantitative manner such accuracy:

- *False rejection rate* (FRR). It is the percentage of eligible user requesting access declared by the system as non-eligible;
- *False acceptance rate* (FAR). It is the percentage of non-eligible access attempts identified as valid users.
- *Equal error rate* (ERR). The point at which FRR and FAR are the same.

Additional comparative analysis of the same biometrics systems used in Table 1, provide the following measures from the accuracy point of view.

Biometrics	FRR	FAR	EER	References
Fingerprint	2.2%	2.2%	2.2%	[Ca06], [Bi06]
Signature off-line	10-30 %	10-30%	10-30%	[KSX04], [YJX07]
Voice	5-10%	2-5%	6%	[Re05], [PM04]

Table 2. Accuracy performance of biometric systems

Based on the values shown in table 2, fingerprints are again, the best positioned biometric characteristic. However, as we will explain in the definition of our proposal, fingerprints do not give any advantage over the current solutions on remote registration environment. Furthermore, voice biometrics behave better than handwriting signatures. The values for voice have been obtained by using a telephone communication [Re05].

2.3 Preventing Multiple Registration on Biometric Systems

Another issue detected during the study of the current remote registration systems is the capacity to detect multiple registers from the same voter. To analyze how biometric systems can manage this issue, we considered the two main operation contexts implemented by biometric systems for user authentication: verification and identification.

Verification. In this context, the system verifies a user identity by comparing the given biometric data with a template stored in the system database. To start the comparison, the user gives a personal ID or username known by the system. The system then retrieves the template related to such user and carries out a one-to-one comparison. That way it is possible to determine if a user is who she claims to be.

Identification. In this context, the user does not need a personal ID or username. Based on the biometric characteristic given by the user, the system has to identify if such characteristic corresponds to one stored in its database. In this case, a one-to-n comparison is carried out.

Based on the operation of both contexts, we can identify that current remote voter registration methods only use the verification context; registration officers use voter personal information to retrieve the signature stored in their database for the comparison. However, using a biometric system in the identification context, the signature of the register could be checked against the complete database of signatures stored. Then, in case the same voter attempts to register more than once using different personal information, she will be detected. Therefore, the use of an identification context prevents multiple registrations by voter.

2.4 Binding Biometrics and Contents

Finally, in order to overcome the feasibility of an attacker changing the contents of a registration form, or separating such contents from the voter identification element, it is necessary to get a link between the contents of the registration form and the voter identification element.

Nowadays, a usual method to protect information is the digital signature. A digital signature protects the information from alterations and binds such information to its author. However, digital signatures have important logistic problems, for example it is necessary for a PKI to generate and provide users with digital certificates.

On the other hand, despite the advantages that biometrics can give to the identification or verification aspects, not all the biometric techniques provide a bind between the biometric characteristic and the contents of a message. For example, in the comparisons presented, fingerprint is considered the most efficient biometric in the values scale given. However, neither fingerprints nor signatures, are usable for binding the contents. In both cases the contents of a message can be manipulated and this cannot be detected by means of the fingerprint or signature.

We have evaluated how to take advantage from the most usable biometrics to carry out the voter registration process in a more effective way. The main idea, as we already have mentioned, is to bind the contents of the registration form to the identification element (i.e. the biometric characteristic). Table 3 shows a new element (hand-writing) and a new requirement (content binding). The handwriting element is added as an extension of signature. Handwriting refers to the unique characteristics that an individual posseses in his or her writing. The new requirement added in table 3 refers to the ability to bind the contents, in our case registration information, to the biometric characteristic. Note that both signature and writing have the same values in the initial compared requirements. However, writing biometrics as well as voice possesses that peculiar characteristic, which is the binding that can give between the biometric characteristic and the contents of the message. In the proposal, we take advantage of such binding to improve the current registration systems.

Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Robustness**	**Content binding**
Fingerprint	H	H	H	M	H	M	M	No
Signature off-line	M	M	L	H	L	H	L	No
Handwriting	M	M	L	H	L	H	L	Yes
Voice	H	M	M	H	M	H	L	Yes

Table 3. An extended comparison of biometric characteristics

3. Proposal

This proposal carries out a remote voter registration in a secure way. It protects from alterations the contents of the voter registration information by binding such information to the voter identity. This is reached by means of combining biometrics and cryptographic techniques that do not require a public key infrastructure. It consists of creating a kind of biometric digital signature. That means a biometric characteristic that can give at the same time both authentication and integrity to the contents.

The scenario for the application of the scheme is a voter registration over Internet. However, other application scenarios are currently possible.

In this scheme, four participants are necessary during the voter registration process: a citizen requesting to be a voter, a registration module, a validation module and the registration officer.

Voter- The voter provides her personal data in order to generate the registration information. The voter also will collaborate to generate a registration proof based on both, her biometric characteristic and the registration information.

Registration module- This module is used to enter the voter registration information and generate an integrity proof of such registration information.

Validation module- The registration proof is generated by means of this module. Such proof is generated with the biometric information provided by the voter.

Registration officers- The registration officers receive the voter register information and carry out some validation processes.

The scheme is divided in two main stages:

- Introduction of the voter registration information and protection of the integrity
- Generation and validation of a registration proof

Based on this division the scheme behaves as follows.

3.1 Introduction of the Voter Registration Information and Protection of the Integrity

The voter connects to the Web site of the Registration Module by means of a secure and encrypted channel, e.g. SSL. The Web site provides a registration form. The voter fills out the registration form with his or her required personal data. Once the registration form is completed, an integrity proof is generated by the Registration Module. Such integrity proof is a cryptographic hash function of the registration information provided by the voter.

The integrity proof is then represented in a format that can be legible by the voter, for instance, a base-32 notation [RFC06]. We selected base-32 notation instead of others available notations (e.g., base-64) for usability reasons: it uses a reduced set of characters focused on minimizing interpretation mistakes. For example, the number 0 is not included in the representation set to prevent being confused by the letter "O."

This representation is shown to the voter by means of the same communication channel. Figure 1 shows the interaction between the voter and the Registration Module to carry out the remote registration and get the integrity proof.

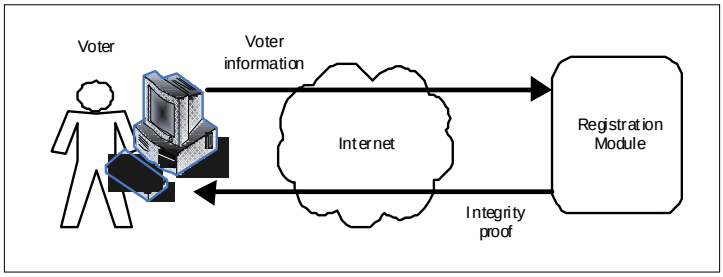


Figure 1: Interaction between Voter and Registration Module

In order to get the integrity proof it is used as a combination of MD5 and SHA1 hash functions. The latest is used in its MAC implementation. This combination is conceived with the aim of preventing collisions between the digest messages, such as was found in the last years for MD5 [Ha04, Kl05, Wa05, WY05] and for SHA1 [Wa05, WY05]. The integrity proof generation is then as follows:

1. Get a digest k from the registration information M_i:

$$K = \text{MD5}\ [M_i]$$

2. Use k as a key to get a HMAC-SHA1 from the same registration information M_i:

$$H = \text{HMAC-SHA1}\ [M_i, K]$$

The resultant H is the integrity proof.

Using a combination of MD5 and HMAC-SHA1, the probability to have a collision decreases significantly. An attacker needs to find a coincidence of collision for the same text on both systems. In addition, we are reducing the probability of these collisions without increasing the size of the digest that remains the same as a SHA1 (160 bits).

Since *H* is based on an HMAC-SHA1, it is 160 bits long, i.e. 2^{160} different digests. Therefore, a base-32 notation (which is 2^5) allows a representation of SHA1 in 32 characters. These 32 characters can be shown to the voter in six groups of five characters plus the two remaining ones. However, the integrity proof *H* can be truncated in order to give a higher usability. For example, taking only the first 20 characters, they can be shown in five groups of four characters or four groups of five characters, which is usable enough.

To prevent reply attacks, each form has a unique number. Therefore, two forms with the same contents will always have different integrity proofs.

Finally, the form with the voter register information and integrity proof is sent to the registration officers. This can be done by posting the on-line registration form or by printing and sending it by a postal service. The preferred option is using an on-line channel, since it allows the implementation of cryptographic techniques that cannot be applied on a postal delivery (e.g., encryption of the information). The received information is stored by the registration officers pending for further validation.

3.2 Generation and Validation of a Registration Proof

The second stage is the generation of a registration proof and the validation of the registration information. Based on the previous analysis, we will use a voice biometric system in this stage.

The voter carries out a communication with the Validation Module. This communication is done by means of a phone call. Then the voter is asked to give the integrity proof. He or she speeches the proof previously shown by the Registration Module, i.e. the groups of characters that represent the integrity proof. By doing this process, the voice of the voter is bound to the contents of the registration information. This is called the registration proof. The registration proof is then stored by the Validation Module. Figure 2 shows the interaction between the voter and the Validation Module in order to generate the registration proof.

The registration proof protects the integrity of the registration information. Any change in the registration information causes the registration proof to not correspond to the contents of the registration information. The registration proof also binds the contents of the registration information to the author, that is, the voter who provides his or her personal information.

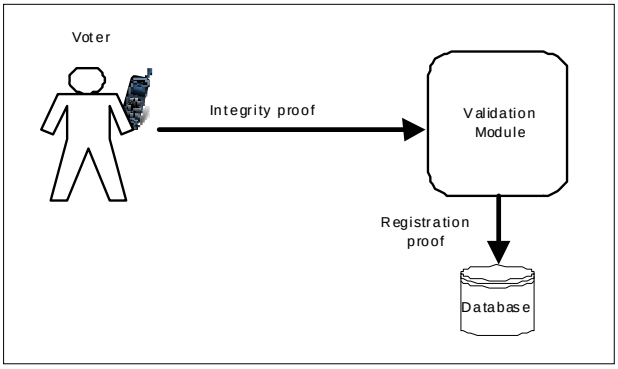


Figure 2: Interaction between Voter and Validation Module

The interaction between the voter and the Validation Module includes, besides the speech of the integrity proof, other dynamic data in order to prevent reply attacks in which an attacker could use a pre-recorded voice of a voter. Such dynamic data could consist of a challenge to the voter who has to repeat a word or a set of words said by the Validation Module. That way, the Validation Module can be sure that the integrity proof is being spoken by a person who is on the other side of the communication line and not by a pre-recorded or automatic process.

Once the registration officers have recorded the validation proof, they can start the validation process.

The validation process facilitates the detection of people who attempt to create more than one record. It is possible to compare the voice of a voter who is validating a new registration with the set of voices previously recorded. That way, a person attempting to create a bogus or an additional record will be rejected, and the registration information associated with the proof provided by such a person will be identified as invalid. Therefore, the probability of impersonation is low. This verification is not necessarily carried out on-line but it can be made after the registration process.

Since any attempt at creating bogus records can be detected through the validation process, the scheme does not require a previous database with the recorded voice of voters. However, for future registrations, the previous records can be used in order to validate the voice of the voter who is making the new record.

An additional validation consists on checking the voter registration information against the associated registration proof. This check will consist on verifying if the integrity proofs match. That means, if the hash of the voter registration form has the same value as the one recorded as part of the registration proof.

If registration proofs and voter registration records pass all the validations, election officers can accept the voter registration information of the voter. If any of the validations fail, the voter registration form and corresponding registration proof can be classified as non-validated records. Therefore, registration officers can implement additional manual checks or contact the voter for checking the process if required.

In a subsequent voting stage, it could be possible to use the registration proof to verify that the person who is voting is the same who created the registration information by checking his or her voice.

Our scheme can be also used as a means to activate the voter credentials once they have been received by the voter. This is usable if the voter credentials are sent to voters by remote means. In such cases, there is the risk that voter credentials are received or intercepted by a third person. The activation technique prevents somebody using the voter credentials instead of the legitimate voter. The activation is carried out by means of an activation code, which is enclosed to the voter credentials. The voter has to call and say the activation code to the registration authority and then a process of comparison between the activation voice and the voice recorded during the registration process is carried out. If the activation voice is the corresponding one, then the voter credentials are validated and authorized to participate in the election. That way, an illegitimate use of the voter credentials is prevented.

Another possible scenario in which our voter registration process can be applied is by using handwriting biometrics instead of voice. The first part of the process (generation of the registration information and integrity proof) could be the same as the previously described, that is, through Internet. The second part of the process (generation of the integrity proof) is carried by the voter by writing by hand the representation of the integrity proof. That way, the registration proof binds the contents of the registration information with the handwriting biometrics of the voter. The handwriting of the integrity proof is carried out in a form provided by the election authority. Once filled out by the voter with the hand-written integrity proof, this form is sent to the election authority by means of postal mail. The sending can be also by electronic means such as fax or e-mail. In the case of electronic sending, the form has to be previously converted to a digital format by scanning it. Even when the verification of a writing text is as difficult as the signature verification, the advantage of the writing text respect to the signature is that it can do the linking to the contents as we have explained before.

4 Conclusions

Current remote voter registration systems have important issues that can facilitate voter impersonation. These issues are mainly voter identification accuracy, multiple registrations from the same person and voter registration information integrity. In this paper we proposed the use of biometrics systems to increase the voter identification accuracy of voters that make a remote registration. In addition, operating on an identification context, biometrics systems can automate the detection of multi registrations made by the same person. Finally, we identified and proposed some biometrics methods, such as handwriting and voice biometrics that can also bind the registration information to the voter identity. Combining this later feature with the use of cryptographic algorithms, such as hash functions, we also provided a way to protect the integrity of voter registration information that can be suitable to implement in current environments.

References

[Ac04] Acquisti, A: Receipt-free homomorphic elections and write-in ballots, Cryptology ePrint Archive, Report 2004/105, http://eprint.iacr.org/, 2004.

[Bi06] Biometric System Laboratory - University of Bologna: "FVC2006: The Fourth International Fingerprint Verification Competition," 2006. Available at http://bias.csr.unibo.it/fvc2006/default.asp.

[Ca06] Cappelli, R. et. al.: Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, January 2006.

[De06] Department of Defense U.S., Report on IVAS 2006, As Required by Section 596 of the National Defense Authorization Act for Fiscal Year 2007, December 2006.

[El07] Election Law Blog. The Extremely Weak Evidence of Voter Fraud in Crawford, the Indiana Voter ID Case. May, 2007. Available at http://electionlawblog.org/archives/008378.html

[El08] Electoral Commission' website to register to vote. Available online at http://www.aboutmyvote.co.uk/register/CitzSelect.cfm?officeID=214&CFID=12799012&CFTOKEN=71181288

[Fv08] FVAP Voting Assistance Guide. Available online at http://www.fvap.gov/pubs/vag.html#ch3

[Ha04] Hawkes, P. et. al.: MD5 collision, October 2004. Available at http://eprint.iacr.org/2004/264.

[Ho07] Hof, S.: E-Voting and Biometric Systems? Electronic Voting in Europe. pp. 63-72. 2004.

[JR04] Jain, A.; Ross, A.; Prabhakar, S: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, pp. 4-20, January 2004.

[Kl05] Klima, V.: Finding MD5 collisions on a notebook PC using multi-message modifications. In International Scientific Conference Security and Protection of Information, May 2005.

[Kr07] Krivoruchko, T: Robust Coercion-Resistant Registration for Remote E-Voting, Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007), 2007.

[KSX04] Kalera, M.; Srihari, S.; Xu, A.: Offline signature verification and identification using distance statistics. International Journal of Pattern Recognition and Artificial Intelligence, Vol. 18, No. 7 pp. 1339-1360. 2004.

[PM04] Przybocki, M.; Martin, A.: NIST, Speaker Recognition Evaluation Chronicles. In Odyssey: The Speaker and Language Recognition Workshop, pp. 12–22. Toledo, Spain, May 2004.

[Re05] Reynolds, D. et. al.: The 2004 MIT Lincoln laboratory speaker recognition system, in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing, Philadelphia, PA, March 2005.

[RFC06] RFC 4648. October 2006. Available at http://tools.ietf.org/html/rfc4648#section-6

[Sc06] Schweisgut, J: Coercion-resistant electronic elections with observer, 2nd International Workshop on Electronic Voting, Bregenz, August 2006.

[Ti06] Tiltont, C.: The Role of Biometrics in enterprise Security. Dell Power Solutions. 2006. Available online at http://www.dell.com/downloads/global/power/ps1q06-20050132-Tilton-OE.pdf.

[Wa05] Wang, X. et. al.: Cryptanalysis of the hash functions MD4 and RIPEMD. In Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings (2005), vol. 3494 of Lecture Notes in Computer Science, Springer, pp. 1-18.

[WY05] Wang, X.; Yu, H.: How to break MD5 and other hash functions. In Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings (2005), vol. 3494 of Lecture Notes in Computer Science, Springer, pp. 19-35.

[YJX07] Yu, Q.; Jianzhuang, L.; Xiaoou T.: Offline Signature Verification Using Online Handwriting Registration. Computer Vision and Pattern Recognition, CVPR '07. IEEE Conference on. pp. 1-8. June 2007.

Long-term Retention in E-Voting – Legal Requirements and Technical Implementation

Rotraud Gitter[1], Lucie Langer[2], Susanne Okunick[3], Zoi Opitz-Talidou[1]

[1]Universität Kassel
– provet –
Wilhelmshöher Allee 64-66
34119 Kassel, Germany
{r.gitter | z.talidou}@uni-kassel.de

[2]Technische Universität Darmstadt
Cryptography and Computeralgebra
Hochschulstraße 10
64289 Darmstadt, Germany
emailadresse@autor1
langer@cdc.informatik.tu-darmstadt.de

[3]pawisda systems GmbH
Robert-Koch-Straße 9
64331 Weiterstadt, Germany
susanne.okunick@pawisda.de

Abstract: Legally binding elections require retention of specified election data such as balloting material. This applies to paper-based as well as electronic elections. However, in Germany, legal requirements on retention in e-voting have not been issued so far. Based on the German legal framework for governmental as well as non-governmental paper-based elections, we give recommendations on long-term retention in e-voting, applying our results to a state-of-the-art e-voting scheme. We also review technical measures to meet the security requirements of long-term retention in e-voting.

1 Introduction

In the context of governmental actions and democratic elections especially, secure long-term storage is an important issue. Strict regulations apply here and compliance with these obligations must be documented as a proof of correct process implementation. Turning to e-government and e-voting in particular, new challenges have to be faced in this area: While the classical paper-based form of documentation just needs to be stored in a safe place once and for all, long-term retention of electronic data truly is a long-term task. Electronic data can easily be changed, therefore issues like integrity and authenticity must be addressed. Furthermore, due to hardware and software obsolescence, difficulties in terms of readability emerge.

With respect to democratic elections, the ballots must be retained over a specific period (usually several years) to allow recounting in case of contestations. Hence, for legally binding elections there exist legal obligations regarding long-term retention. This applies to common paper-based as well as electronic elections. But unlike the paper-based variant, legal regulations for remote electronic elections have not yet been issued in general. In its recommendation on legal, operational and technical standards for e-voting [Cou04], the Council of Europe states that “the e-voting system shall maintain the availability and integrity of the electronic ballot box," which means that “the information kept in the electronic ballot box must be securely saved for as long as this is necessary to permit any recount or legal challenge or for the period after the election required by the electoral process in the member state in question" [Cou04, Standard No. 99]. Concrete measures are a matter for national legislature. The German Informatics Society (Gesellschaft für Informatik – GI) has developed a catalogue of requirements for online elections in non-governmental organizations [Ges05], presuming that there exist no regulations regarding long-term retention of election results. At the same time, the GI as well as the German Research Foundation (Deutsche Forschungsgemeinschaft – DFG) have adopted their own regulations for online elections, which comprise also regulations regarding long-term retention of election records (cf. [Ges04], [Deu06]).

The different issues of long-term retention in general have been addressed by a lot of research projects. The projects nestor [nes] and PADI [PAD] brought together and made available competences and information regarding technical, organizational, and legal aspects of long-term archiving. InterPARES [Int] is a major international research initiative that aims at developing the knowledge necessary to provide policies, strategies and standards capable of ensuring the longevity and trusted authenticity of digital material. In Germany the DOMEA concept [DOM] defines requirements for document management and electronic archiving in e-government. The long-term conservation of electronically signed documents has been addressed by the European Telecommunications Standards Institute [ETS03] and the projects ArchiSig [Arc] and TransiDoc [Tra]. The LTANS group [LTA] brings forward the standardization in this area. However, long-term retention in the context of e-voting has not yet been addressed before and the question as to which data should be retained is unanswered. [VK06] focuses on the challenge of providing everlasting privacy for online elections that, at the same time, are based on cryptosystems that may be broken at some point in the future. But to the best of our knowledge, long-term retention in the case of electronic elections has not yet been studied thoroughly before.

Our paper is structured as follows. In Section 2 we review the regulations for paper-based elections in Germany and transfer them to online voting, providing legal requirements regarding long-term retention of election data in e-voting. In Section 3 we apply our results to a state-of-the-art e-voting protocol and evaluate which data must be retained in particular to meet the legal requirements we have derived. Following a more technical approach, we report on specific requirements regarding retention in e-voting in Section 4: Which security objectives must be achieved? Which measures should therefore be applied? We also provide concrete recommendations regarding the technical implementation, referring to the protocol we have analyzed in Section 3. Concluding remarks are given in Section 5.

2 Legal Framework

In the following we analyze the legal regulations that apply to selected election types in Germany, reaching from governmental elections for democratic decision-making to non-governmental elections in civil society.

2.1 Legal Requirements for Conventional, Paper-based Elections

Parliament.

Elections of the German Bundestag take place every four years [Sch98]. They are subject to the Federal Electoral Law (Bundeswahlgesetz – BWG) and specified by the Federal Election Ordinance (Bundeswahlordnung – BWO), which contains provisions for documentation and safekeeping of the election material. According to Art. 72 BWO, the election board has to keep a record of the election process, the vote counting and the election results. Discarded ballot papers must be enclosed in the record as well as envelopes and polling cards whose validity has been questioned. The record has to be approved and signed by the members of the election board. All documents are handed over to the municipality hereafter. The municipal authorities have to retain the election documents for a period determined by Art. 90 BWO. Protection against unauthorized access must be ensured. The following election documents have to be retained for six months, as long as no scrutiny procedure is pending and no law enforcement authority needs to investigate regulatory offences: the electoral roll, the polling card register, the register of invalid polling cards, and the register of persons (for example in hospitals or monasteries) who according to Art. 29 (1) BWO, were allowed to vote by a moving election board; furthermore, the form letters containing the signatures assisting the nomination of candidates. All the other documents such as voting papers, voting envelopes, and the documents of the postal vote have to be retained in accordance with Art. 90 (3) BWO for the whole legislative period of the Bundestag, until 60 days before the elections of a new Bundestag.

The longest retaining period for elections documents amounts to four years. This period may be extended if pursuant to Art. 49 BWG scrutiny procedures are pending or when regulatory offences (see Art. 107-108e StGB) need to be investigated by the law enforcement authorities. Consequently, the appropriate election documents may be needed for a period of longer than four years to be used as evidence material for the hearing or the proceedings.

Works Council.

Elections of the works council are held every four years. The election process is governed by Art. 7-20 of the German Works Constitution Act (Betriebsverfassungsgesetzes – BetrVG) and, in detail, determined by a special election ordinance (Wahlordnung – WO). Documentation requirements are stipulated in Art. 18 BetrVG, Art. 16 and 19 WO. According to Art. 18 (3) BetrVG the election board has to establish a record of the election process subsequently to the termination of the election. The record must contain the total of the ballot envelopes handed in, the total of valid and invalid votes, the number of valid votes for every list of candidates, the distribution of seats to the lists, the names of the elected candidates, and finally, any incidents or matters that might affect the validity of the election. The record must be signed by the chairman and at least one different member of the election board (*writing requirement*). According to Art. 19 BetrVG an election may be contested if any of the essential rules regarding the right to vote, eligibility or the electoral procedure have been infringed and no subsequent correction has been made. In this case only infringements that verifiably could not have altered or influenced the election results will not affect the validity of the election. As a rule, contestations must be filed within two weeks of the announcement of the election results.

However, severe infringements exceptionally may be claimed even hereafter, whereupon the election result might be declared void at any time. Art. 19 WO therefore stipulates that the newly elected works council has to retain all relevant election documents at least until the end of its term of office. These documents are, in addition to the record of the election board, any other documents in the broadest sense that might be relevant in case of election contest: for example ballots, announcements of the election board and the envelopes of late postal votes that were not counted.

Governing Boards of Social Security Institutions.

Elections of the governing boards of the social pension funds as well as for the health, nursing and accident insurances take place every six years. The election process is governed by Art. 43 et sqq. of the Social Security Code (SGB IV) and by the special Electoral Ordinance for that sector (SVWO). According to Art. 91 SVWO there is a general obligation to retain the election documents for the whole term of office of the governing boards. However, the voter's election pass, the ballot papers, the ballot envelopes and the postal voting envelopes can be discarded if the election is not contested one month after the announcement of the final results (see Art. 57 (3) SGB IV). In case of an election contest, these documents have to be retained for at least two months after the court decision has become legally binding, as far as no special reasons demand further retaining.

Executive Committee of an Association.

The executive committee of an association is elected at the annual general membership meeting [Kur04]. The election procedure is organized pursuant to the provisions of Art. 28 et sqq. of the German Civil Code (BGB), if the articles of association do not stipulate something else (Art. 40 BGB). Details of the electoral procedure, for example the voting principles, the eligibility requirements, or the modality of the election performance, may be regulated according to the discretion of the body setting down a separate voting statute of the association [Rei07].

On the association level, elections have already been carried out electronically: The German Informatics Society as well as the German Research Foundation have issued their own e-voting statutes (cf. [Ges04], [Deu06]). Both of them comprise provisions concerning the retention of electronic election documents and the voting software which provide for a retention period according to the term of office of the executive committee, i.e. two and four years, respectively.

2.2 Obligations for Documentation and Retention in E-Voting

Legal rules governing elections demand a thorough documentation of the election process and the retrieval of the results. Even if it is not explicitly stipulated (as for the elections of the executive committee of an association), a preservation of these documents is necessary to prove the dual process of the election and the correct calculation of results. As a rule these documents should be stored at least for the term of office of the elected body. E-Voting systems must provide for an appropriate electronic documentation to prove the compliance with basic voting principles. The election host therefore must be able to demonstrate how the technical or organizational processes which could alter or influence the election results work in general and if the system functions properly. For this purpose the election host must be able to prove the security of the relevant components and applications of the voting system. The tallying process must be verifiable and hence repeatable. Thus, in particular the number of cast and counted ballots – including the number of valid and invalid ballots – must be documented, as well as logging files that can exclude any manipulation of the system. It should be possible to recount the election results by a trustworthy counting program. If legal norms require paper-based documentation (e.g. for the record of the election board), printouts can be generated and signed by the responsible authority. According to German law, it is also possible to replace the handwritten signature by a qualified electronic signature. In any case, qualified signatures should be used to provide for the integrity and authenticity of the electronic documentation [Siga].

3 Implementing Legal Requirements: A Concrete Example

In the following, we apply our results regarding legal stipulations on long-term retention to the e-voting scheme designed by Juels, Catalano, and Jakobsson (JCJ) [JCJ05]. First we give a short description of the protocol. Hereafter we investigate which of the occuring data must be retained in order to meet the legal requirements we have identified in Section 2.

3.1 Protocol Description

The scheme proposed by JCJ was the first one to offer coercion-resistance, which means that a voter cannot be forced to abstain from voting or to vote in a particular way. In effect, a potential adversary cannot learn whether the coerced voter complied with his demand. To achieve this, the JCJ scheme is designed such that the identity of the voter remains hidden during vote-casting and validity of the ballot is verified by blind comparison against an electoral roll. For this, secret anonymous credentials are distributed among the voters during registration phase. These credentials serve two purposes: Firstly, they are employed for authentication and authorization of the voters. Secondly, they mark a "free" vote in the sense that this vote indeed expresses the voter's will; if a voter wants the vote to be accounted, she includes her valid credential. If she casts the vote under coercion, she attaches an invalid credential. The coercer is not able to distinguish invalid credentials from valid ones and hence cannot know if the voter has complied with his demand. Since multiple voting is allowed, the voter can hereafter cast a valid vote. In the end, only the latest vote with a valid credential is accounted in the tallying process.

Registration.

The identity and eligibility of each voter is first verified by the registration authority. Upon successful verification, voter v_i receives a unique valid credential σ_i from the registration authority over an untappable channel. An encrypted version S_i of this credential is published on the bulletin board. At the end of registration phase, the electoral roll L contains all valid encrypted credentials alongside the plaintext names of registered voters and is signed by the registration authority. The registration authority is assumed to be trustworthy, but can also prove to a voter that σ_i is authentic, i.e. that S_i is a valid encryption of σ_i. However, it must be assumed that the registration authority does not leak credentials to an adversary.

Voting.

The registration authority publishes an integrity-protected candidate list *C*. For voting, the voter v_i casts a ballot over an anonymous channel. The ballot comprises the following parts:

1. A probabilistic encryption of the chosen candidate c_j, hereafter referred to as the *vote*

2. A probabilistic encryption of the voter's credential σ_i

3. A non-interactive zero-knowledge proof (cf. [BSMP91]) that c_j is in C

4. A non-interactive zero-knowledge proof of knowledge of σ_i and c_j

Voter v_i encrypts her valid credential σ_i if she wants her vote to be accounted, otherwise she encrypts a fake credential σ_i'. The proof that c_j indeed marks a valid candidate is necessary since casting write-in votes could compromise coercion-resistance. Knowledge of σ_i and c_j must be proved to prevent replay-attacks by simply re-encrypting votes that have already been cast.

Tallying.

1. Proof checking. The tallying authority first checks that all proofs included in each ballot are correct. Ballots containing invalid proofs are discarded. For all the remaining ballots, let A_1 denote the list of encrypted votes and B_1 the list of encrypted credentials.

2. Duplicate removal. Next, the tallying authority removes ballots with credential duplicates via plaintext equivalence test (see [JJ00]). Only the latest credentials in B_1 are kept, resulting in a weeded list B_2. The ciphertexts in A_1, which correspond to duplicate credentials are also removed, resulting in a weeded list A_2. Now there is no more than one vote per given credential.

3. Mixing. The list of encrypted votes as well as the list of encrypted credentials is mixed using the same, secret permutation.

4. Validity checking. The credentials from B_2 are compared with the ones in L via plaintext equivalence test, eliminating those which do not correspond to valid credentials in L. The corresponding invalid votes from A_2 are eliminated as well. Let A_3 and B_3 denote the final lists. These now correspond to authentic ballots cast freely by eligible voters with no more than one vote per voter.

5. Vote counting. Finally the votes in A_3 are decrypted and tallied.

3.2 Meeting Legal Requirements

We now investigate which data should be retained in order to meet the legal obligations specified in 2.2. Here we only specify *which* data is to be stored. Comments on the question *how* this should be done will be given in Section 4.

First of all, the list L is to be kept; it denotes the eligible voters and contains their valid, encrypted credentials. Furthermore, the list C should be stored since it contains the names of the candidates including unique identifiers used for vote-casting.

Let N denote the total number of ballots cast in the election. This value includes also multiple ballots cast by single voters under valid as well as invalid credentials. In 2.2 we have stated that that the number of cast and counted ballots – including the number of valid and invalid ballots – must be documented. Hence, we first have to determine what "invalid" votes actually are with regard to the analyzed voting scheme. As mentioned before, for the JCJ scheme to remain coercion-resistant, it is excluded that voters cast write-in votes, which means that they vote for candidates that are not on list C and hence are invalid. This implies that voters cannot cast invalid votes, i.e. ballots that have been invalidated by the content of the vote and not by using an invalid credential. A ballot can thus only be invalid for one of the following reasons:

(a) It contains an invalid proof

(b) It has been cast under a valid credential, which was later on re-used to vote

(c) It was cast under an invalid credential

The number of ballots corresponding to the these categories are the following:

(a) $N - |B_1|$ (see phase 1 of the tallying procedure)

(b) $|B_1| - |B_2|$ (see phase 2 of the tallying procedure)

(c) $|B_2| - |B_3|$ (see phase 4 of the tallying procedure)

According to 2.2 the retrieval of the election result shall be documented, which includes also ballots that have been declared invalid. In particular, ballots that contain invalid proofs and hence are to be discarded in phase 1 of the tallying procedure should not be deleted but rather kept for retention and just eliminated from the tally. For being able to exclude replay attacks, the valid proofs of knowledge of the tallied votes should be kept as well.

Subtracting the number of invalid ballots specified above from the total of N ballots gives $N - (N - |B_1| + |B_1| - |B_2| + |B_2| - |B_3|) = |B_3|$ valid ballots. This is no surprise since B_3 contains the valid, unique credentials under which votes have been cast. This list should be retained, as it must be verifiable that only eligible voters have cast a ballot.

Re-tallying of the votes requires retaining list A_3 since it contains encrypted votes, which correspond to the valid, unique credentials in B_3.

Besides protocol-specific data we have just considered, additional material must be retained. According to the legal stipulations, it must be provable that the system functions properly and no manipulations have been performed. System auditing files as well as logging files of intrusion detection systems in use should therefore be retained in addition to the material specified above.

4 Technical Implementation of Long-Term Retention

In this section we address the technical realization of long-term retention. First we appoint the technical requirements for electronic and electronically signed voting material to meet legal obligations. Next we outline suitable technical protection methods. Finally we apply the results to the scheme proposed by JCJ, which we have introduced in Section 3.

4.1 Requirements for E-Voting

General requirements for the technical implementation of long-term retention are specified in [RFDJ07] and [WPB07]. In the following these requirements are transferred to e-voting:

Integrity. Any kind of retention is targeted at preserving the integrity of a document, i.e. preserving it as it originally has been created. Undetected modification or deletion of any election document, in particular the electronic ballots, must be prevented. Integrity – and hence the whole election – is compromised otherwise.

Authenticity. The authenticity of the documents must be preserved to keep the originator of the document identifiable. In case of electronic elections, special attention must be paid to the task of ensuring authenticity of the ballots (e.g. confirmed by a validating authority) on the one hand while providing for strict anonymity of the vote on the other hand.

Completeness. Since the whole election process has to be documented, the connection of the single election documents should be preserved.

Confidentiality. Voting material containing personal data of the voters must be protected against unauthorized knowledge. For instance the voter's signature includes the voter's certificate, which may contain sensitive personal data of the voter.

Negotiability. A document is negotiable if it is possible to transfer it if from one system to another without losing the possibility to check the characteristics of the document, for example, its integrity. In case of contestations, the evidential voting material has to be presented before the court without any quality loss.

Readability. The voting documents have to be readable, i.e. hardware to access the stored data must be available as well as software to interpret and present it. We assume that permanent availability of the voting data during the retention period is not required.

4.2 Technical Protection Methods

In the following, we present existing technical protection methods and evaluate them on the basis of the requirements defined above. The protection methods are divided into the following categories according to [RFDJ07]:

System-oriented. Data access is controlled by a technical system. By configuring the archiving system accordingly, access is restricted to certain components or persons. An example is write protection on a file system defining groups with reading and writing privileges.

Medium-oriented. This category includes storage media for which the overwriting or manipulating of the stored information is not possible, e.g. WORM (write once read many) or other non-rewritable media.

Document-oriented. This comprises technologies to preserve documents against unauthorized extraction of content and undetected modifications, for example encryption and qualified signatures.

In [RFDJ07] some protection methods out of every category are evaluated. At this point we pick up this evaluation and work out recommendations for the retention of e-voting documents.

Using Qualified Signatures.

As mentioned in Section 2 qualified signatures should be used to provide provability of the integrity and authenticity of the election documentation. A qualified signature proves that the data has not been modified and ensures that the originator of the signed document can be identified.

Signatures are also a suitable method to ensure completeness and negotiability. Completeness may be guaranteed by pooling all voting documents and signing this collection. Furthermore, a signed document is negotiable because any third person is able to verify the signature and thus prove the integrity and authenticity of the document. In contrast to signatures, system-oriented methods limit the negotiability of a document: An unsigned document protected by access control in a given system loses this protection when given to a third party. The third party is not able to verify the integrity of the document and has to trust the applied system or must verify its security.

Using Well-Known, Standardized Signature and Data Formats.

To ensure negotiability, accepted or standardized data formats should be used. If a rare and unknown format is used, the court will have to consult an expert opinion, which may cause great costs. Well-known or standardized signature formats are:

1. CMS (Cryptographic Message Standard) [Hou04]

2. XML signatures [ERS02]

3. PDF/A (ISO 19005-1:2005, this ISO standardization of the PDF/A specification includes the electronic signature)

General usage of standardized formats increases the probability that appropriate software is available and hence contributes to long-term readability.

Access Restriction During the Retention Period.

As previously mentioned, qualified signatures conserve the provability of signed documents, but they do not protect against modifications during the retention period. Therefore, additional protection methods are necessary. Suitable are non-rewritable media or system-oriented methods for the file system, document management systems or archive systems where the document is stored, e.g. access control software or a read-only mode for the documents. An alternative is the usage of any portable storage media as DVD or USB, which are deposited at a place accessible only by authorized persons. By access restriction the confidentiality of retained sensitive voting data can be achieved as well.

Redundant Data Management.

In general it is useful to hold the data redundant to safeguard against loss in case of unexpected impacts such as theft or fire. For this purpose, backups should be provided and kept in at a different place.

4.3 Long-Term Aspects

The retention period has great influence on the realization of retention since all technical protection methods are subject to an aging process and require an update. In the following we select long-term aspects important for e-voting.

Generally, obsolete archive systems and storage media have to be replaced by state-of-the-art technologies. During the replacing process data must not be modified or lost. We assume that currently available hardware that meets the minimal quality standard is durable for the expected retention time in e-voting.

In the case of electronic signatures, an aging process applies as well. After a certain time, the underlying cryptographic algorithms and parameters become insecure. Thus signatures lose their integrity and authenticity and hence their probative value. This process may be significant after six years and therefore concerns signed e-voting documents. In Germany, according to §6 of the Signature Act [Siga] and §17 of the Signature Ordinance [Sigb] electronic signatures have to be renewed by a new qualified electronic signature before the used algorithms lose their security suitability. In the concept of signature renewal the new signature is performed by a time stamp. A time stamp is issued by a time stamp service, which signs the document after adding a date. In the ArchiSig project [Arc] a concept has been developed in which a lot of documents are renewed by one time stamp [RS06]. At first the documents are merged in a hash tree in accordance with Merkle [Mer80]. Then a time stamp for the root hash value of the tree representing all documents is requested. This procedure is independent of document formats and more cost-efficient since qualified time stamps usually require a fee. The concept complies with the German and European Signature Law [Roß04]. The LTANS group [LTA] brings forward the standardization in this area, cf. [BPG07]. However, only few products exist which handle signature renewal.

E-Voting protocols such as the JCJ scheme mentioned in Section 3 usually employ encryption to ensure confidentiality. The aging process of cryptographic algorithms also influences the encrypted data. With the decreasing security suitability of the used algorithms, the encrypted document loses its confidentiality. Therefore additional measures should be taken during the retention period to ensure confidentiality.

4.4 Applying the Results to the JCJ Scheme

Finally, we briefly comment on long-term retention methods for the JCJ scheme discussed in Section 3.

While, for example the electoral roll L is supposed to be signed by the registration authority, most of the other data which is to be retained such as the lists A_3 and B_3 are a priori not signed. However, it is not sufficient to store the data unsigned since both data integrity and authenticity has to be provable before the court. Therefore it is inevitable to sign the material. Signing all lists including L by one authority additionally proves the completeness of the voting material. As recommended in Section 2, qualified signatures should be used.

To ensure negotiability, a non-proprietary format should be chosen for the lists. Otherwise the lists can only be interpreted and presented by appropriate proprietary software. To prove the compliance with essential voting rules, the security of the software must be examined. To ensure confidentiality, the encrypted credentials in the lists have to be protected against unauthorized access before the encryption parameters and algorithms become insecure.

5 Conclusion

Long-term retention is an important issue in e-government and e-voting in particular. Electronic elections can only become legally binding if legal obligations on long-term retention are met. We have transferred the legal regulations on paper-based elections in Germany to the scenario of online elections, providing guidelines for long-term retention in e-voting. Following an exemplary e-voting protocol we have analyzed which data must be retained concretely. We have also provided technical requirements for retaining voting documents and recommended technical protection methods. Our work shows that the requirements of long-term retention should be taken into account already when designing an e-voting protocol or selecting a scheme to be used for a practical implementation. We believe that we hereby contribute to building the foundations of e-voting and help advancing online elections, not only in Germany.

References

[Arc] The ArchiSig Project. http://www.archisig.de/, last checked 26.02.2008.

[BPG07] Ralf Brandner, Ulrich Pordesch, and Tobias Gondrom. Evidence Record Syntax (ERS). RFC, 4998, August 2007. http://www.ietf.org/rfc/rfc4998.txt, last checked 25.02.2008.

[BSMP91] Manuel Blum, Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Noninteractive Zero-Knowledge. SIAM J. Comput., 20(6):1084–1118, 1991.

[Cou04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11, September 2004. http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/, last checked 13.02.2008.

[Deu06] Deutsche Forschungsgemeinschaft. Wahlordnung für die Wahl der Mitglieder der Fachkollegien der Deutschen Forschungsgemeinschaft (DFG), 2006. http://www.dfg.de/forschungsfoerderung/formulare/download/70_01.pdf, last checked 25.02.2008.

[DOM] DOMEA-Konzept. http://www.kbst.bund.de/cln_011/nn_836960/Content/Standards/Domea_Konzept/domea_node.html_nnn=true, last checked 28.02.2008.

[ERS02] Donald Eastlake, Joseph Reagle, and David Solo. (Extensible Markup Language) XML-Signature Syntax and Processing. RFC, 3275, March 2002. http://www.ietf.org/rfc/rfc3275.txt, last checked 26.02.2008.

[ETS03] ETSI TS 101 733 V1.5.1, 2003.

[Ges04] Gesellschaft für Informatik. Ordnung der Wahlen und Abstimmungen, 2004. http://www.gi-ev.de/fileadmin/redaktion/OWA/gi-owa.pdf, last checked 24.02.2008.

[Ges05] Gesellschaft für Informatik. GI-Anforderungen an Internetbasierte Vereinswahlen ("GI requirements for Internet based elections in non-governmental organizations"), August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf, last checked 13.02.2008.

[Hou04] Russ Housley. Cryptographic Message Syntax (CMS). RFC, 3852, July 2004. http://www.ietf.org/rfc/rfc3852.txt, last checked 26.02.2008.

[Int] The InterPARES Project. http://www.interpares.org/, last checked 25.02.2008.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, WPES, pages 61–70. ACM, 2005.

[JJ00] Markus Jakobsson and Ari Juels. Mix and Match: Secure Function Evaluation via Ciphertexts. In Tatsuaki Okamoto, editor, ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, pages 162–177. Springer, 2000.

[Kur04] Kurt Stöber. Handbuch zum Vereinsrecht. Otto Schmidt, München, 2004.

[LTA] Long-Term Archive and Notary Services (ltans). http://www.ietf.org/html.charters/ltans-charter.html, last checked 26.02.2008.

[Mer80] Ralph C. Merkle. Protocols for Public Key Cryptosystems. In IEEE Symposium on Security and Privacy, pages 122–134, 1980.

[nes] nestor – The German Network of Expertise in Digital Long-Term Preservation. http://www.langzeitarchivierung.de/index.php? newlang=eng, last checked 28.02.2008.

[PAD] PADI – Preserving Access to Digital Information. http://www.nla.gov.au/padi/, last checked 28.02.2008.

[Rei07] Bernhard Reichert. Vereins- und Verbandsrecht. Luchterhand Verlag, 2007.

[RFDJ07] Alexander Roßnagel, Stefanie Fischer-Dieskau, and Silke Jandt. Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, August 2007. http://www.bmwi.de, last checked 25.02.2008.

[Roß04] Alexander Roßnagel. Signaturgesetzkonformität des Standardisierungsvorschlags "Long-Term Conservation of Electronic Signatures" für die ISIS-MTT Spezifikation vom 30.6.2004, July 2004. http://www.teletrust.de/fileadmin/files/ag8_isis-mtt-gutachten-langzeitsig.pdf, last checked 28.02.2008.

[RS06] Alexander Roßnagel and Paul Schmücker. Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit? Economica Verlagsgruppe Hüthig Jehle Rehm GmbH, Heidelberg, 2006.

[Sch98] Wolfgang Schreiber. Handbuch des Wahlrechts zum Deutschen Bundestag. 1998.

[Siga] German Electronic Signature Act (Gesetzliche Rahmenbedingungen für elektronische Signaturen, SigG). http://bundesrecht.juris.de/sigg_2001/index.html, last checked 13.02.2008.

[Sigb] German Electronic Signature Ordinance (Verordnung zur elektronischen Signatur, SigV). http://bundesrecht.juris.de/sigv_2001/index.html, last checked 13.02.2008.

[Tra] Legally Secure Transformations of Signed Documents. http://www.transidoc.de, last checked 20.01.2008.

[VK06] Melanie Volkamer and Robert Krimmer. Online-Wahlen und die Forderung nach zeitlich unbegrenzt geheimen Wahlen. Working Paper Series on Electronic Voting and Participation, 02/2006, 2006.

[WPB07] Carl Wallace, Ulrich Pordesch, and Ralf Brandner. Long-Term Archive Service Requirements. RFC, 4810, March 2007. http://www.ietf.org/rfc/rfc4810.txt, last checked 25.02.2008.

Session 4: Comparison of E-Voting

The E-Voting Readiness Index

Robert Krimmer, Ronald Schuster

E-Voting.CC
Competence Center for Electronic Voting and Participation
Pyrkergasse 33/1/2, A-1190 Vienna, Austria
{r.krimmer | r.schuster}@e-voting.cc

Abstract: The goal of this study is to analyse and compare the environment for the introduction of E-Voting. To do so a contextual model is developed and then applied with the value benefit analysis to compare 31 countries including all EU member states, and Russia, Switzerland, United States and Venezuela.

1 Introduction

The use of information and communication technology (ICT) in the electoral process is continuously rising around the world. While most of the applications emerge in the back-office, hence the administration of the election like electronic electoral registers or mandate calculate, ICT is finally reaching the home of the voters.

As can be seen in international gatherings of E-Voting experts, the discussion around is led very actively. The use of E-Voting machines has taken up in many countries, the uses of E-Voting in remote elections is in contrast still small in size [KTV07].

So far there has been only one study by Leenes and Svensson which could not identify a unique trend for the adoption of E-Voting other than that it is dependant from the context [LeSv03].

In the following we will introduce the methodology and give some first findings of our study.

2 Methodology

For our analysis of the E-Voting context, we needed on the one hand the contextual model where we identified the necessary dimensions to be used, and on the other hand the methodology to assess the countries.

2.1 Contextual Model

For the development of a contextual model for E-Voting we could use previous work, namely the work by Leenes/Svenson [LeSv03] and Moosmann/Baumberger [MoBa03]. These were integrated in our first approach as described in [Krim04], where four dimensions were identified: the political, legal, technological and social dimenions. These factors constitute the national (macro) level in contrast to the process (micro) level for the concrete application under investigation. These dimensions were also broken down in subdimensions.

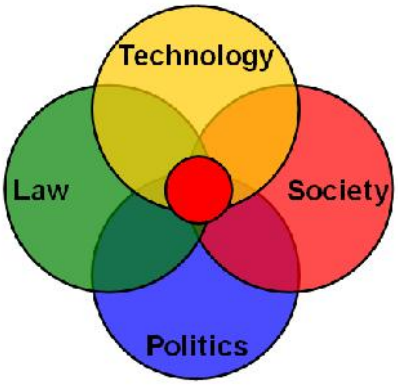


Figure 2: The Dimenions of E-Voting

We then extended this model using Pippa Norris's view [PiNo01, 11] where she distinguishes among three nested levels of analysis, as illustrated in figure 3. The national context, including the macro-level of technological, socioeconomic, and political environment, determines the diffusion of the Internet within each country. These three environments are similar to those from the previous model. The institutional context of the virtual political system provides the structure of opportunities mediating between citizens and the state, including the use of digital information and communication technologies by governments and civic society. Here the political process takes place. The individual or micro-level of resources and motivation determines who participates within the virtual political system. Norris' framework assumes that the national context, such as the process of technological diffusion, influences the development of the virtual political system. In turn, the core institutions of the political system available in the digital world provide the systematic context within individual citizens have opportunities to participate online. It is determined by the particular citizen, personal resources (time, money, skills) and their motivation to take advantage of these opportunities.

The final model consists of two levels to be explored:

- National level (Macro)
- Application level (Micro)

While the national level handles with E-Democracy environment in general, the level on project basis examines the application E-Voting. Regarding E-Democracy, the dimensions on the national view level which can be considered are divided as figure 3 shows:

- Information Society Context
- Political Context
- Legal Context Information

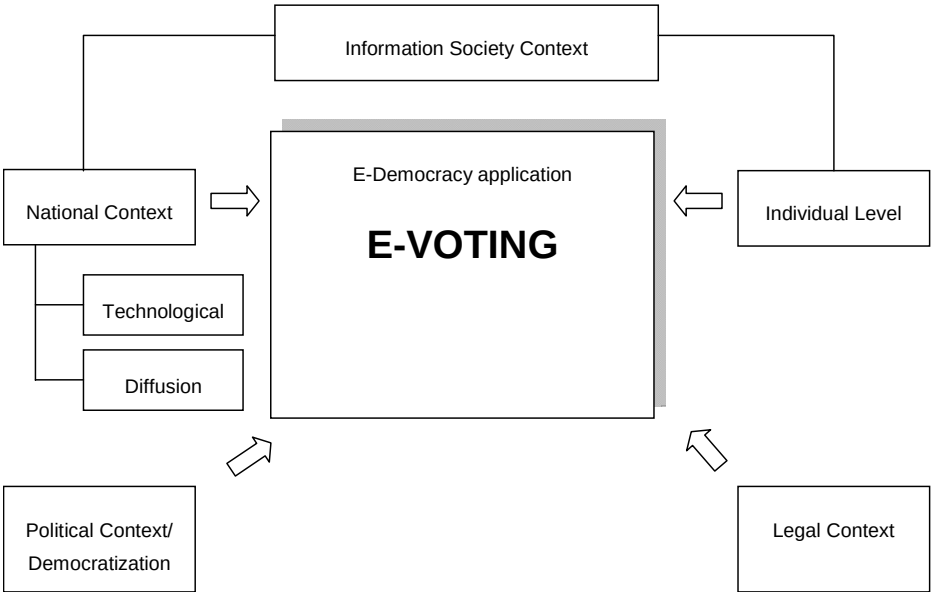


Figure 3: The E-Voting Readiness Index Contextual Model [RoSc07, 16]

The "information society context" is divided into "national context" and the "individual context" of the users whereby the latter is not considered in this work. The "national level" is further divided into "technological" and "diffusion". In this dimension there are items like computer penetration, internet penetration to be measured as E-Democracy is an IT topic.

The "political context" considers the democratization of a country by measuring subdimensions like "institutional stability" or "stateness". A stable democracy is necessary for the introduction of E-Democracy applications like E-Voting.

The "Legal Context" measures basics for democratic elections like election system or supplementary protocol for human rights that are required by a democracy.

Those dimensions that are relevant for E-Democracy have a great impact on a possible application like E-Voting. The result of the first stage “national view level” can be considered as an E-Democracy readiness scale.

The second stage to be measured is the application level with the application E-Voting that is influenced by the environment. This stage is divided into public and private projects to guarantee that individual experiences are not mixed with the development progress of the state and completes the E-Democracy readiness scale of the first stage to a complete E-Voting readiness scale.

For each of the dimensions numerous weighted indicators have been found that were grouped to weighted subdimension that are summed up to the dimensions. By summing up the weighted dimensions the E-Voting readiness can be explored.

The next table shows the dimensions and it’s subdimensions used.

	E-Democracy Environment			Application E-Voting
DIMENSIONS	Information Society Context	Legal Context	Political Context	E-Voting Applicaton
SUBDIMENSIONS	Status of registers	Election System	Stateness	Public debate
	Status of eGovernment infrastructure	Supplementary protocol for human rights	Rule of law	Private elections
	Digital net infrastructure	Realization of Council of Europe recommendation	Stability of democratic institutions	Public elections
	Prices for the entrance to information and communication service and for the use of services		Election system and turnout	
	Diffusion of information and communication services		Politicial participation	
	Expenditures for information technologies and information and communication-referred services		Political aims	
	Transaction penetration			
	Degree of the informatization in the public administration and of administrative expirations			

Table 1: The Factors for the E-Voting Readiness Scale

2.2 Methodology

The requirement was to find a method that allows the analysis of different opportunities to reach a defined goal. Zangemeister's basic system of the value benefit analysis turned out to be useful setting up our methodology. He regards his method as analysis of a quantity of complex alternatives with the purpose of arranging the elements according to the preferences of the decision maker. Phases proposed are: (i) Definition of situation-relevant goals, (ii) description alternatives to reach a goal, (iii) a preference order of the alternatives due to the goals that have to be achieved. [Zang76, 45]

Using the value benefit analysis it becomes possible to include the non quantifiable use into an evaluation with and thus to eliminate the main difficulty creating costs using comparisons. We used the more specified approach from Stahlknecht and Hasenkamp [StHa05] who applied the value benefit analysis for assessing tenders in the IT-sector.

1. Listing and weighting of the criteria. The criteria relevant from the view of user are arranged and weighted proportionally. The sum of the weighting results in 100 percent.

2. Confrontation of the units of analysis. The units are confronted on the basis of the selected criteria.

3. Evaluation and scoring of the units of analysis. Each unit is evaluated regarding each criterion. The values are then multiplied according to the associated weights and the final values are added. Thus result into the individual utilizable value of the alternative.

We adapted this approach for our purposes as follows:

1. The superordinate goal is the development of the E-Voting readiness scale. In order to develop this scale, the relevant environmental dimensions must be identified (see 2.2).

2. Dimensions are divided into thematically matching subdimensions. These sub-dimensions contain the individual indicators. Each indicator is evaluated on a four-level scale, whereby alternative 1 describes the least favorable environment situation and therefore gets only 0,25 points and alternative 4 is the most favorable environment situation and gets 1 point.

3. Since the individual indicators do not have the same importance for the evaluation of a subdimension, these are weighted. The sum of the weighted criteria results in a number for the subdimension.

4. The subdimensions are weighted too as their contribution to the utilizable value for the dimensions are different. The sum of the weighted subdimensions is a number for the whole dimension expressing the utilizable value for the environment of the whole dimension.

5. Finally the different dimensions have to be weighted according to their importance of contribution to the E-Voting readiness. The sum of the weighted dimensions results in a number that expresses the E-Voting readiness.

The following figure represents this procedure.

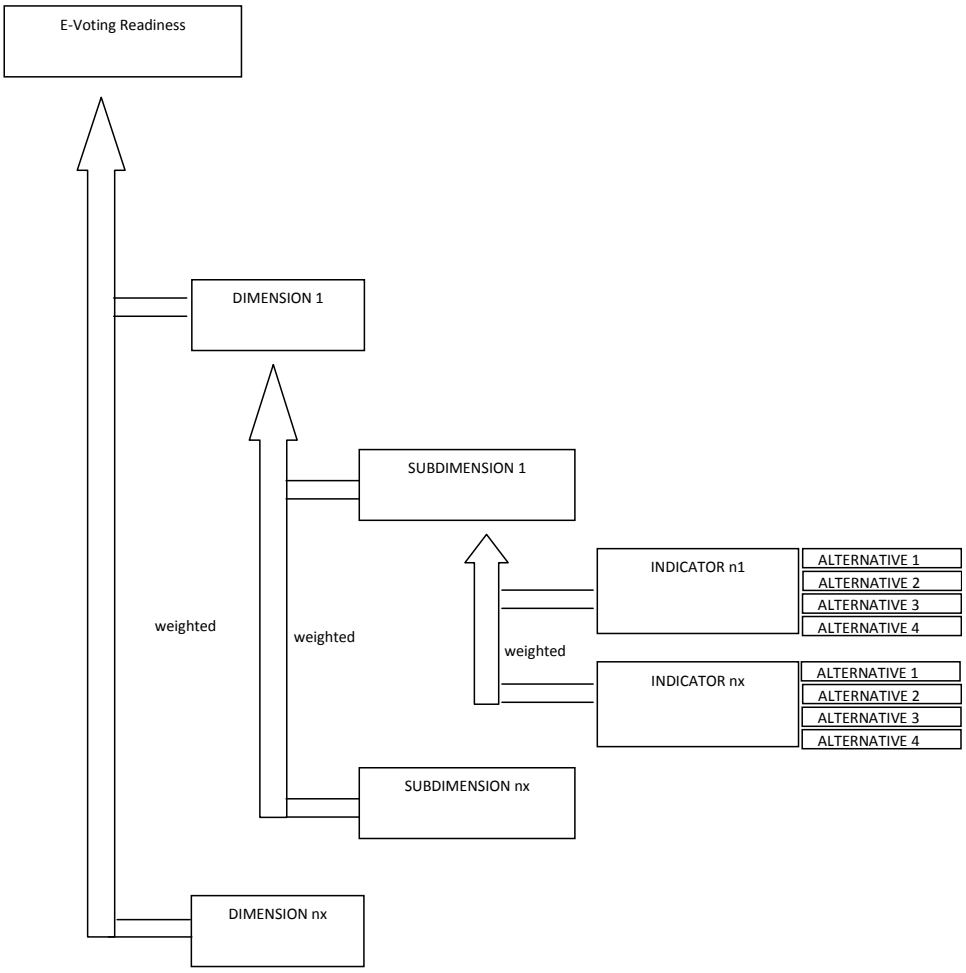


Figure 1: The Evaluation Procedure for the E-Voting Readiness Scale following the Value Benefit Analysis

3 Study

We used the above described methodology of a value benefit analysis together with the contextual model to answer our main question, which is to measure the progessiveness of countries in preparing the right context for E-Voting. To do so, we developed factors for each of the subdimensions to determine and measure the criteria. In the end we had 79 single factors (Political Context: 16, Legal Context: 10, Information Society Context: 29, E-Voting: 24). The next step was the weighting of the (sub) dimensions, and factors. We weighted the E-Voting with 40% and each of the three macro levels with 20%.

In the next step we identified 31 countries for the study. We included all 27 member states of the European Union, as well as relevant countries with E-Voting experiences where data was available: Russia, Switzerland, United States and Venezuela. The research team was extended by IT experts with native language skills and then used desktop research to collect the data and assessed the factors between 0,25 to 1.

As an example we will walk you through the process of classifying relevant dimensions with the example of Great Britain.

In order to be able to evaluate specific items we consulted research articles, press releases, experts and different sources in the World Wide Web. All data were collected twice. If we had divergences in data material we started further investigations.

The political context of Great Britain is well developed. Indicators evaluating the fields of constitutional state, stability of democratic institutions, political participation and political aims were scored at highest levels. We found restrictions in election turnout.

The legal context of Great Britain shows an excellent environment for E-Voting. We did not find any restrictions in the election system. There is no postal voting implemented, but advanced voting exists.

Concerning the IS context the major findings were: No citizen register is implemented. The voting register is organized de-central and electronically. Registration procedure for elections is the responsibility of government authorities. Digital signature is available. A Citizen card is considered to be introduced soon. E-Government standards are implemented. Indicators for penetration of computers, internet and mobile phones show values of 44.8 percent, 67 percent and 109 percent. Further internet transactions like online shopping and e-Government applications have been executed on a high level by citizens shortly below 40 percent. Just eight percent handle their finances electronically.

Great Britain tested all kinds of electronic voting: Voting machines, kiosk voting and I-Voting. There have been private electronic elections. Politically binding elections fulfill the comprehensive British experience: Voting machines in polling stations, kiosk voting and remote electronic voting.

The study resulted in the following weighted factors according to the four dimensions:

	Political	Legal	InfSoc	E-Vote	Total
Austria	19,58	14,20	14,04	12,13	59,96
Belgium	20,00	11,40	10,20	15,35	56,95
Bulgaria	15,33	8,40	4,17	1,47	29,37
Cyprus	14,58	8,40	5,19	0,00	28,17
Czech Republic	18,23	8,40	8,05	2,37	37,05
Denmark	20,00	17,00	8,99	8,55	54,54
Estonia	17,88	16,76	14,36	17,60	66,60
Finland	19,08	14,20	10,64	12,87	56,79
France	19,50	8,40	9,23	19,53	56,66
Germany	19,50	14,20	10,37	15,00	59,07
Greece	18,88	8,40	6,45	7,50	41,23
Hungary	19,00	8,40	9,41	2,50	39,31
Ireland	18,90	10,40	6,63	6,93	42,86
Italy	16,10	8,40	7,76	14,80	47,06
Latvia	18,00	8,40	4,76	3,47	34,63
Lithuania	17,00	8,40	5,23	5,47	36,10
Luxembourg	20,00	11,20	10,17	0,37	41,74
Malta	19,40	11,40	4,44	3,10	38,34
Netherlands	20,00	14,20	8,80	19,90	62,90
Poland	17,67	8,40	4,89	2,92	33,87
Portugal	19,00	11,20	7,92	14,92	53,04
Romania	15,38	8,40	4,97	5,13	33,88
Russia	13,57	8,40	5,61	10,30	37,88
Slovakia	15,27	16,30	6,07	6,57	44,20
Slovenia	19,00	11,20	6,01	4,35	40,56
Spain	18,08	8,40	9,44	17,43	53,36
Sweden	20,00	17,00	11,39	11,50	59,89
Switzerland	19,00	14,00	10,39	18,40	61,79
United Kingdom	19,15	11,50	8,60	31,35	70,60
United States	18,50	16,30	8,18	23,70	66,68
Venezuela	11,68	8,40	6,88	11,60	38,57

4 Conclusion

This project was an ambitious effort to the development of the contextual model and to collect the data. However the collected data and analysis will provide for a better understanding of the environment for E-Voting and in consequence it will benefit future research in the area. The future work will concentrate on finding significant relations between contextual factors and successful deployment of E-Voting.

References

[PiNo01] Norris, P.: Digital Divide, Civic Engagement, Information Poverty and the Internet Worldwide, Cambridge University Press, Cambridge, 2001.

[Krim04] Krimmer, R., Die Dimensionen der elektronischen Demokratie, in: Proceedings of IRIS 2004, Verlag Österreich, Salzburg 2004.

[KTV07] Krimmer, R., Triessnig, S., Volkamer, V.: The Development of Remote E-Voting around the World: A Review of Roads and Directions. In: Alkassar, A., Volkamer, M.: VOTE-ID 07, Springer LNCS, 2007.

[MoBa03] Moosmann, R., Baumberger, P.: E-Voting-Sicherheitskonzepte - eine vergleichende Studie (2003), Egovernment Präsenz, Zeitschrift des Institut für Wirtschaft und Verwaltung, Vol., 02, 2003.

[RJSB03] Leenes, R., Svenson, J.: ICT in the Voting Process - A Report on 17 European Countries: University of Twente, 2003.

[RoSc07] Schuster R.: Development of an e-Voting Readiness Scale, Diploma Thesis, Vienna, 2007.

[StHa05] Stahlknecht P., Hasenkamp. U.: Einführung in die Wirtschaftsinformatik, (11th Ed.), Springer, Berlin – Heidelberg 2005.

[Zang76] Zangemeister, C.: Nutzwertanalyse in der Systemtechnik, (4th Ed..), Wittemann, München, 1976.

Malfunction or Misfit: Comparing Requirements, Inputs, and Public Confidence Outcomes of E-Voting in the U.S. and Europe

E. John Sebes, Gregory A. Miller

Open Source Digital Voting Foundation
665 Lytton Ave., Palo Alto, CA, USA
http://osdv.org
{jsebes | gmiller}@osdv.org

Abstract: While European democracies are increasingly adopting e-voting technology – including remote voting via public networks – the e-voting experience in the U.S. has been one of disenchantment. The adoption of e-voting technology and outcomes in public confidence in elections processes and results are at significant variance between the U.S. and Europe. We argue that the causes of this variance are rooted in divergent inputs of political traditions that only loosely define systems requirements. In the case of the U.S., several factors, most notably balkanization of the elections processes, have led to the current situation where e-voting technology is a poor fit for unclear systems requirements that are only now becoming clearly understood. A comparative analysis of European and U.S. experiences is the basis for a solvable problem statement for the U.S. situation, together with a solution approach that is being attempted at present.

1 Introduction

Public confidence in the outcome of the use of digital voting technology (hereinafter referred to as "e-voting") is very different in Europe as compared with the U.S. To take two of a great many examples, Swiss e-voting pilot projects [BB06] showed a dramatic increase in participation, via Web-based remote balloting, of habitual non-voters, while in the U.S. advocacy groups called for a return to non-electronic voting.

This striking difference is not merely a reflection of European technophilia and suspicious American technophobia. To understand what one might call "American e-voting dysfunction" we need to look at the American political tradition and the implicit technical and system requirements in our electoral process. We suggest a developmental model of five parts. Political traditions create often-inconsistent sets of elections process goals that create varying trust models, partially determining election system requirements, that are applied (or misapplied) to defining functional requirements for e-voting.

By comparing the U.S. and Europe in this developmental model, we can show how American e-voting dysfunction is as much a result of engineering misfit as it is of technical malfunctions–and indeed that the latter is a consequence of the former. This account of the technology misfit provides the framework for an approach to correcting e-voting dysfunction. This approach is a combination of developmental process, trust process, and functional fit. In addition to being a framework for the creation of sound e-voting systems, this combination is specifically designed to enable a public process of restoring voter confidence in e-voting as a beneficial (not merely neutral) component of an elections system.

2 From Political Traditions to Elections Process

Regarding elections and trust, the American political tradition in the 21st century is still very much based on experience in the 19th century, in at least these three regards: vote buying and coercion; polling-place election fraud; and election fraud in canvassing. Each of these concerns is not only a lasting concern in the American political tradition, but also a driver for formulation of present-day goals for election process, trust models, and system requirements for e-voting systems.

Vote buying and coercion are the most notable instances of voter fraud that are enabled by the lack of effective privacy for casting ballots. There are many historically documented forms [Ca05], but one example may suffice for purposes of comparison: the notorious role of the "precinct boss." In the polling place of a politically corrupt precinct dominated by one political party, the role of a precinct boss was to observe each voter's ballots to determine whether the voter voted in accordance with previous direction, and hence was eligible for reward or punishment.

Concerns over vote buying and coercion have historically been the drivers for the election process goal of the combination of privacy and anonymity in the voting process. More recently, these concerns have manifested in two ways concerning vote-by-mail. In one view, moving the balloting process away from the precinct polling place eliminates the opportunity for precinct-based organized, scalable ("wholesale") coercion/bribery. In another view, large-scale mail voting enables coercion/bribery for a sufficiently large number of voters as to cast doubt on election result validity, especially in close elections. The latter appears to be the more prevalent position, though the actual incidence of this type of voter fraud is debated [MC03], particularly in the state of Oregon (state-wide vote by mail). As voluntary vote-by-mail participation in California has risen above 30%, it may be that parts of the American West are demonstrating a *wertewandel*, or mutation of values, concerning the link between privacy and coercion/bribery.

Vote-by-mail also shows a potential *wertewandel* concerning anonymity. Currently, a ballot is anonymous, but it may be enclosed in an envelope that identifies the voter. Identification is required to determine whether the putative voter is entitled to vote. This approach suggests that current voters may trust election officials not to correlate ballots and voters, despite their ability to do so.

Two other aspects of concern are forms of election fraud–-one in the polling places (where access to ballots enables the insertion of spurious or fraudulent ballots); and the other as part of the canvassing process, where undesirable ballots are simply not counted. Many examples have been described [AB00] ranging from the canonical "stuffing the ballot box" to accidents in which a block of ballots is mislaid, invalidated, or simply not counted. Suspicions of fraud are raised when historical voting patterns indicate that the missing ballots could be expected to trend against the desire of elections officials.

These concerns essentially describe a lack of trust in elections officials and in the elected office-holders who have authority or influence over them. Perhaps the most notorious recent incident was in the Florida 2000 American Presidential race. Personal and partisan relationships among the Secretary of State (who had oversight of the elections), the Governor of the State, and the ultimate race winner (the Governor's brother) permanently clouded election results. Although this and similar experiences sparked some excellent work on recommended election reforms [Ca02, Cr04], to date little work has been done to look at how e-voting technology can be trusted to support any of the suggested reforms.

2.1 Election Fraud and the Push to Automation

Election automation is perhaps the most striking and uniquely American result from a political tradition of high sensitivity to election fraud. In the late 19th century, states began using electro-mechanical voting machines that led to the lever machines that remained in wide use in some states as late as 2007. The main driver for adoption was the idea that the machines were more trustworthy by virtue of being less easily manipulated by elections officials to perform wholesale election fraud. This type of automation retained a great deal of public trust despite defects of low auditability, no ballot of reference, no paper trail, etc.

European countries certainly also have histories of election fraud, and real concern over how to structure elections to control it. However, the US may be unique in the degree of mistrust that creates a preference for automation over "pure manual" elections of hard-marked, hand-counted paper ballots.

2.2 Comparison of Election Goals

The elements of American political tradition drive a number of goals for elections processes: privacy of balloting; anonymity of balloting; minimization of distrust in both elected officials and elections officials; auditing and transparency of canvassing and other actions of elections officials. These goals in turn serve as drivers for trust models and systems requirements for e-voting. These goals – and how they define elections processes and technology – exist in marked contrast between the U.S. and many European countries, especially those that make greater use of e-voting. There are two distinct types of contrast: hearty adopters, and non-adopters of e-voting.

In the hearty adopter category are Estonia and parts of Switzerland. Many Swiss cantons have been encouraging vote-by-mail for some time in order to increase voter participation. Although, as noted above, vote-by-mail can create some concerns about anonymity and distrust of elections officials, neither of these values is as strongly held in the Swiss political tradition. Indeed, historically, non-anonymous town-square voting, e.g., a show of hands, was viewed as a traditional value for high-confidence elections.

Similarly, the anonymity concern over vote-by-mail seems largely absent, particularly with the extension to "Internet voting." The high rate of participation in pilots, especially among habitual non-voters, shows a significant trust in elections officials' proper use and dissemination of e-voting data. Anecdotal evidence from elections officials indicates pilot participants were not concerned about privacy, or at least correlation of voter identification and ballot. Participants in the pilot similarly trusted the technology involved, including the PCs, Web browsers, Web applications, the public Internet for communications, and Web application security standards for communication security. A similar set of values is indicated in the Estonian Internet voting experience, with the addition of increased reliance on technology for voting authentication and authorization.

In the non-adopter category are the Netherlands and Ireland. The Netherlands is notable for having effectively outlawed e-voting after nationwide adoption approached 100% in March 2006, with the vast majority of municipalities using the same election system. Shortly thereafter, a documented security issue of the system (described in [Gh07]) and public activism resulted in two government commission studies, the first of which reported that many safeguards thought to be essential to verifiable elections had been ignored because the new technology was not properly understood. The second commission's report suggested the possible future use of open source systems for marking and counting paper ballots. The Dutch government acted to revoke its previous legal framework [Ne07] for defining voting machines for use in the Netherlands; subsequent elections have returned to manually counted paper ballots.

Ireland also conducts elections using manually counted paper ballots. The use of e-voting was seriously considered at one time, however. The Irish government created a Commission on Electronic Voting, which reported in 2004 that it could not recommend the use of an electronic system [Ce04]. Later work also failed to provide the basis for e-voting usage in Ireland, and the commission was dissolved in 2006. There seemed to be a lack of sufficient benefit for the cost and risk of e-voting. Although mitigation of electoral fraud was a potential benefit, it should by no means be taken as an indication of Irish indifference to the issue. Rather, Ireland's rather infrequent (5 and 7 year terms mean that 2 years or more can go by between elections) and simple (often one measure and rarely more than five, each separately balloted) elections are subject to the structured process of manual counting with observation by the general public, and political party officials observing to perform independent counting. The structure and the avid observation may be related in part to the non-trivial method of tallying with Ireland's form of the single transferable ballot.

By contrast, the American response to election fraud concerns has included the use of automation. While the particularly weighty American history (a political tradition of voter fraud, election fraud, corrupt elected officials and elections officials, often referred to *in toto* as "machine politics") of fraud may be one factor, the much higher complexity and frequency of elections may contribute as well.

2.3 Election Complexity and the Push to Automation

American election officials may well look with envy on feasibly hand-counted single-contest ballots, with feasible public visibility of counting – even if they are proponents of e-voting. Election complexity arises partly from a more complex governmental structure than many European countries, resulting in more frequent elections with more contests. Yet some European countries have a similar degree of complexity of offices, and have not adopted e-voting – France is perhaps the best example.

Another fact in election complexity is the result of another form of balkanization, coupled with response to another legacy of American "machine politics" – cronyism, nepotism, patronage, and similar ways in which elected officials use their power of appointing government officials, for their own personal gain. This part of the American political tradition has led to a frequent practice of electing officials that in other times or in other jurisdictions were appointed. The balkanization effect arises from the fact that these locally elected offices are for jurisdictions that are not co-extensive with legislative or local jurisdictions. For example, some parts of a county will be in one school district or another; of the parts that are in one school district, one subset will be in a different water district. A not infrequent result is that in some counties, almost every voting place has a distinct ballot with a distinct set of contests. One anecdotal example: by the time the next President of the U.S. is elected, one author will have voted 4 times in 367 days for a total number of contests numbering at least 30 and likely over 40, in jurisdictions that include: multiple county offices and referenda, offices or referenda from at least 3 local jurisdictions (fire district, harbour district, coastal commission), state and federal offices, and all in a "light year" in which municipal offices, state executive officials, and federal senators are not up for election.

In short, a history of fraud has led to a desire to use automation to mitigate the vulnerability of pure manual paper-based elections, while a history of fraud and patronage has led to a high degree of complexity which elections officials are motivated to manage with automation. Pressure from both sides has encouraged automation in the U.S. for over a century, while public trust in the process has eroded in the more recent past. These two trends may help explain why the American election system is problematic regardless of automation, and in a way that drives automation without trust or even a central or consensual model for trust.

3 From Elections Process Goals to Trust Models

Derived from American political traditions, elections process goals in turn drive trust models for elections and for the reflection of them in a digital voting system. To properly understand e-voting trust models, two aspects of the previous statement are critical: the idea of plural models of trust, and a trend toward trust minimization.

First, the plurality of trust models is derived from a fundamental and critical aspect of U.S. elections systems–an aspect which might be called "balkanization." That is, the U.S. Federal government delegates to states the responsibility for Federal elections. States delegate to county elections officials. Each county, therefore, represents a distinct elections body, making its own choices about election processes, with distinct but (typically) limited regulations or guidance from the state. Each state also makes its own elections laws and regulations within a minimal set of Federal requirements. Not only is there no central or standard regulation or guidance on how to conduct elections (and hence what trust properties an elections process should have), the number of variants is at least two orders of magnitude (dozens of counties in many of the 50 states) larger than in European countries with devolved Federal elections, e.g., Switzerland and France. At the far end of the spectrum are unitary democracies in which the central government regulates how municipalities conduct elections, and most contests are for either one level of local government, or for one legislative representative. In the Netherlands for example, it is not uncommon for an election to consist of just one contest.

We would also argue that current U.S. elections are conducted with a distinct default of mistrust, or at least a goal of minimizing trust and increasing transparency and public auditability. The trend seems to be increasingly in this direction, not only in the realm of public advocacy (particularly in the area of verifiable voting) and public opinion, but also of elected officials. For example, California's Humboldt County is one of the counties in which the chief elections official is pursuing transparency by developing a system for capturing electronic images of all ballots and electronically publishing the set of images. At the state level, again in California, the office of the Secretary of State (regulating county elections officials' activity) recently issued a set of guidelines for polling place physical security practices and for an auditable chain of custody of constrained data items items–such as paper ballots and magnetic media–that record electronically cast ballots. Vigorously pursuing these guidelines, only three counties received cognizance of full compliance–and hence the full ability to utilize e-voting in the February 2008 election.

A third factor is complexity of government structure and oversight over elections. In the US, there is often a variety of partisan elected officials (at the local, county, and state levels) who can influence the way an election is conducted. Not only can election integrity appear to be affected by partisan officials, there is a sometimes complex array of such officials. Further compounding the complexity is that in cases of legal dispute, judicial officials may be notably publicly partisan, or may be elected judicial officials who may be seen as not neutral on issues of the election process. Of course, partisan politics also affects public trust in European elections as well. However, in the US, this trust factor is exacerbated by complexity and is combined with the other factors above.

These three characteristics contribute to the lack of a coherent model of trust in our elections process. A model of trust must consider what roles and operations are trusted with what constraints (e.g., in pursuit of anonymity), and associated controls and logging for auditability. Lacking a definitive trust model for an elections process, it is nearly impossible to derive the basis for trust in e-voting systems–systems that automate parts of the existing election process, much less systems that require modification of the existing process. This lack is greatly exacerbated by the range of trust attitudes, e.g., Oregon and California vs. states that attempt to regulate absentee voting.

3.1 Comparison of Elections Process Goals and Trust

European countries are certainly not uniform in centralization of elections functions or regulations over those functions, not even the countries making more extensive use of e-voting. However, some European voting jurisdictions–for example, the country of Estonia [MM05], or the Swiss cantons that implemented Internet-enabled remote voting–have been clear enough about the elections process and trust to be able to implement aggressive (by U.S. standards) e-voting systems with clear technical requirements. The key differentiator (by contrast with the U.S.) is the active role of the voting authorities (national or cantonal) in the implementation of remote voting.

A different contrast to the U.S. is offered by countries that have explicitly rejected e-voting. Irish experience (in selecting, acquiring, piloting, and studying an e-voting system) was driven by the central government empowered to set goals and empanel commissions to assess a system with respect to those goals. The Dutch experience was even more specific, with the central government creating specific regulations defining voting technology for use by municipalities. When it became apparent that the main e-voting system in use did not conform to regulations, and in addition had serious defects out of scope of the regulations, the Dutch government was empowered to retract the regulation (effectively barring e-voting) and empanel studies to recommend policies to be decided by the central government to regulate the entire country.

Both these types of experience could be said to be a successful outcome with e-voting, in that it became clear whether or not available e-voting technology met the goals for its use. The U.S., by contrast, has no such uniform outcome, or indeed any outcome that is stable for multiple election cycles. Unlike the hearty adopters, county elections offices and the offices of Secretaries of State have had low to no direct involvement in the implementation of e-voting systems and the processes that they automate. Rather, these many, many governmental organizations have acted in the role of a traditional consumer of packaged technology, selecting from a few vendors those systems that seemed to best meet state or local needs. One measure of the lack of positive outcome of this approach is the result of the review, performed for the Office of the Secretary of State of California, of all the polling-place and/or canvassing e-voting systems that had previously been certified by the Office for use in California. Reviewed systems were all de-certified, and only three systems re-certified for limited use for accessibility, with a proviso requiring significantly improved physical and procedural security methods and auditing [So03].

Although the grounds for rejection were mainly based on system security and information security considerations, the overarching question is how these systems came to be used in the first place. Further, how is it that in European experiences the systems used were deemed fit to meet their requirements for use, or specifically unfit? We hypothesize that the European experience was more successful because of the existence of a central body which had authority to define or review proposed requirements, the authority and ability to correlate product requirements with trust requirements; the ability to work with technology vendors to obtain e-voting systems that putatively [a] fit the trust model; and b] are a reasonably close fit to overall systems requirements; and the ability and authority to assess and decide whether systems were in fact fit for use in specific terms.

This combination may have enabled either a definitive rejection of e-voting, o a more multilateral and deliberate process of design, implementation and deployment ([Bo06] describes another such example) than is the typical experience in a U.S. county elections office.

4 From Trust Model(s) to E-Voting Requirements

Whether the above conjecture is valid or not, the facts of life in U.S. elections today are that at present no U.S. county or state will be in as advantageous a position as that we conjecture for some European elections bodies. Balkanization, combined with the packaged product model, have created misfit systems, and have not created a profit motive or market incentive for current or new vendors to create revised or new proprietary products that are a better fit. One overarching reason is the number of jurisdictions; it's not feasible for vendors to obtain, let alone satisfy with products, a set of system requirements that meets the needs – including trust – of even a majority of the jurisdictions. Conversely, elections officials in many jurisdictions are oriented to "making due" with available technology under state or Federal deadlines rather than defining requirements and finding systems that fit them.

Given this situation, the misfit of current U.S. e-voting systems is hardly surprising, and certainly not the result of any lack of effort on the part of the vendors. Given no coherent set of goals, let alone requirements, and no model for how the e-voting systems could be trusted, the vendors had little scope for excellence of fit.

Furthermore, the time-to-market motive–particularly for a fixed set of funds allocated to states by the Federal government's HAVA act [Ha02] –resulted in systems where the misfit resulted in visible malfunction, perceived unreliability, or difficulty of administering, and a growing suspicion about security and integrity. The result has been a general decrease in public confidence.

4.1 Comparison of Trust and E-Voting Requirements

As noted above, the more successful efforts in European e-voting have involved systems that were not off-the-shelf devices, but rather systems developed via bespoke systems integration with a significant degree of stated requirements and a trust model that if not explicit, can be derived for the resulting system and the public confidence outcome of using it.

By contrast, the complex and sometimes historically ugly American political tradition has resulted in a large number of jurisdictions that share, to a varying extent, a particular distrust in elections processes and officials, or at least a dominant pessimism about their integrity, combined with a desire for transparency and verifiability. As a result, American e-voting systems are rather a paradox in that the electorate is implicitly expected to trust computers to partially automate elections processes that are themselves not trusted. At the outset, this is a marginally tenable expectation given most voters' less-than-happy experiences with the reliability, integrity, and security of the personal computers they use. Tenability is strained more with the addition of press coverage of voting device insecurity and election technical snafus.

4.2 Approach to Technical Development Towards Public Confidence

At first inspection, the current situation in the U.S., and the comparison with more positive European outcomes of voter experience and public confidence–not only in similar polling-place e-voting scenarios but also in more aggressive remote e-voting–seems unhopeful for marked improvement.

However, the developmental model, and the approach to development within it, suggests that improvement is possible. We do expect initially to develop e-voting systems requirements to match a coherent trust model or set of elections systems goals. Instead, we use a trust framework rather than a single model, and initially develop requirements bottom up from existing elections processes and the non-misfit functionality of existing e-voting systems. The resulting approach is based on three tenets:

1. Despite the lack of a single trust model or a central authority with the means to even vaguely define one, it is possible to create a trust framework that enables both a public process of determining whether specific e-voting systems are trustworthy, as well as a systems development process that can be performed with this trust framework in mind.

2. Existing e-voting systems, in conjunction with a trust framework, can form the basis for deriving election system requirements and functional requirements for specific e-voting devices – especially polling-place devices that are the focus of most of the controversy that strains public confidence.

3. This process and framework require no small efforts to achieve, and the effort is not in the economic interests of vendors or the current operational scope of Federal entities – though some efforts in the latter area may be helpful. However, if the efforts were carried out strictly in pursuit of the public good, and were successful in creating relevant results, then these results could be suitable for adoption and extension by creators of e-voting systems and by Federal and state government organizations with responsibility for elections.

The remainder of this paper describes the trust framework, the method of creating requirements, and the plan for proof-of-concept activities being undertaken by the Open Source Digital Voting Foundation (hereinafter "OSDV").

5 "Trust Framework" Defined

The OSDV approach defines a trust framework in a way that is fairly conventional for high assurance dedicated systems, such as aerospace systems, military systems, and other high-integrity or high-security systems that are fixed-function, dedicated or embedded systems. We observe that many types of e-voting systems (including, but not limited to polling place devices) are or should be fixed function systems that could be trustworthy.

The foundational definition is that a trustworthy device or system does all and only what it is designed to do. A trust framework enables assurance that a particular system is in fact trustworthy. For any particular system, the goal of a trust framework is to be specific about the functions a system is supposed to perform, and how that system could be independently assessed as performing only and all of those functions. The elements of a trust framework are:

Specifications: specific, prescriptive written documentation that defines a particular system and its functions. An implementation of such a specification could be trustworthy if it could be assessed as being conformant to the specification, performing all and only the functions in the specification. As an example of a high-assurance system specification, some Common Criteria Protection Profiles could be considered a specification in this sense. Some U.S. military system "Concept of Operations" documents are good examples of documents that capture a portion of what constitutes a high-assurance specification.

Reference Implementations: a set of hardware and software that implements the specification or a documented subset of the specification, typically with expediency taking priority over other commercially relevant properties. Rapid prototypes of a reference implementation can help to clarify the specification. Even partially complete reference implementations can provide a working example of a trustworthy system, both for proof-of-concept and illustration for others' work on a complete system.

Assessment Guidelines: documentation that specifically describes a methodology for evaluating an implementation of a particular specification. The process of independent assessment is used to evaluate whether a given implementation meets the specification and satisfies other aspects of high assurance, such as software quality. Assessment guidelines are required to enable consistency of assessment efforts across multiple assessments of a system type, and across the efforts of multiple assessors.

Open Assessment Work Examples: Documentation of methods used, findings, results, and overall judgment supported thereby, as a result of the efforts of a complete assessment. System assurance assessments can only assist in building trust and public confidence if the process is transparent and the results are publicly available and vetted. Worked examples of assessment efforts and findings, even undertaken on partial reference implementations, can have a beneficial effect on the clarity of guidelines documents, and serve as a proof-of-concept of the level of effort and feasibility of assessment of a particular specification using corresponding guidelines.

The OSDV approach is to apply this traditional trusted systems approach with related high-assurance systems methodologies to the specifications, reference implementations, open assessments, and documentation of methodologies for e-voting systems. Existing products can serve as the basis for the functional descriptions that are components of a specification for existing product types.

Such efforts have begun on a common system platform for a variety of types of e-voting systems. Platform efforts will be validated in a parallel project to develop e-voting systems based on it, starting with a ballot-scanning device. These efforts are initially focused on polling place devices –as these have caused the most publicly visible effects on voter confidence–but are not intended to be limited to them.

6 The Future: Feasible Development and Assessment of Trustworthy Systems

Assuming that the above efforts are fruitful as envisioned, how might the efforts and results have a markedly positive impact on the current American e-voting dysfunction? One major impact would be to enable a transparently refereed and government supervised evaluation process, similar in some ways to both Common Criteria evaluations performed by today's CCTLs, and to the voting system assessments currently performed for vendors by 3rd parties, in a new program operated by the U.S. National Institute for Standards & Technology (NIST) at the behest of the U.S. Elections Assistance Commission (EAC) [Ea07]. The former types of efforts are standards-based, but intentionally broad and can be burdensome and expensive. The latter are specific to e-voting, but lack public visibility, and cannot be shown to produce consistent results because there are no documented, commonly used (or de-facto standard) system specifications or assessment methods. The OSDV approach will produce results that can fill those gaps in some significant measure.

It is conceivable that in the future, states' certification efforts could be based on the results of transparent, independent evaluations that are feasible and consistent as a result of using standard system specifications and assessment guidelines, together with assessment findings reviews. These standards would be based on OSDV work product, which would have been already proven as usable by other OSDV results in reference implementation, worked example assessment, and public demonstrations. Certainly, the appropriate standards bodies could develop similar standards, but the authors hope the OSDV can fairly quickly develop and validate its work with rapid prototyping and parallel development. The authors envision the OSDV results to be usable during a standards process that would be much shorter as based on the OSDV results than starting afresh with standards committees. We also expect the OSDV results to be complementary to (or in some cases re-use or incorporate by reference) the results of existing work, most notably the U.S. EAC VVSG [Tg07] and work in the U.S. ACCURATE Project [Ac07].

Toward this future, the OSDV Foundation plans to have its reference implementations undergo third party assessment, as well as state certification. Leveraging these results, the OSDV technology transfer plan includes a monetary motivation for others (commercial or public entities) to adopt OSDV technology as the basis for future products: the use of existing, already evaluated platform and core application functionality. This type of adoption could enable product assessments that focus only on extensions outside of the evaluated platform, and be performed more rapidly and cheaply than evaluations of entire systems or revisions to entire systems.

7 The Present: A Digital Public Works Project

Given that vision of future impact, we can describe the current work of the OSDV Foundation as being similar to public works projects and having the following characteristics: based on requirements gathered from existing elections processes; starting from a "blank slate" of functional and trust requirements, without the need to be based on any existing e-voting system; developed transparently in the public eye for the public good, without the motives of commercial gain; performing specification, documentation, prototyping, and assessment efforts in parallel with feedback among these efforts; producing results with proof-of-concept and working examples to validate results. Based on the characteristics, the goal is to deliver proof-of-concepts systems that are developed and documented to be clear about (a) supporting, enabling, and not detracting from election systems requirements discussed above; and (b) the extent and limits of trust required and assumed in the operational environment.

Given these characteristics, we expect OSDV results to provide for the development of systems that could demonstrably support multiple combinations of election system requirements, as well as some well-defined models of trust allocated between technology, practices, physical security, audit, etc.

8 Summary

By comparing European and American experiences, we have argued that current e-voting dysfunction in the U.S. is not based primarily on the use of systems that malfunction due to poor quality, but rather from using commodity systems that are the result of a sometimes hasty and sometimes nearly requirements-free process of development and deployment. Such systems are misfit for their usage and environment because they fail to meet some unstated trust and integrity requirements that might have been derived from a coherent set of trust model and elections process goals–if such a set existed. In the U.S., however, there is no single trust model or single set of explicit (regulatory and legal) requirements, or implicit (operational and design) requirements, but rather a plethora of them. As a result, experience with misfit e-voting technology has drained U.S. public confidence in elections, and created an untenable situation with respect to trust of integrity in e-voting systems.

We have described a partly abductive approach in which we derive system and trust requirements and developmental methodology, by reasoning backwards from both fitting and mis-fitting characteristics of current e-voting devices. We have related this approach to existing misfits, malfunctions, and press coverage that have raised an already high bar in the U.S. (compared with Europe) for trust in elections processes and automation of them. We have described a trust framework and high assurance development methodology that is intended to meet that high bar of trust, and provided a potential model for adoption of OSDV work in that framework.

The overarching goal for adoption is enabling increased U.S. public confidence in e-voting technology and elections in jurisdictions that choose to use high-assurance trustworthy e-voting technology. These intended results will not necessarily be an immediate fit for the needs of a large number of U.S. jurisdictions. However, OSDV results can provide a concrete basis for credible claims of trustworthy systems (a milestone in e-voting in itself), and for iteration of functional requirements to meet specific jurisdictional needs. In addition, the basis for iteration, combined with explicit functional and trust requirements, could further enable some convergence of requirements in multiple jurisdictions, mitigating some effects of the large number of U.S. counties and states.

References

[AB00] Glenn C. Altschuler and Stuart M. Blumin, Rude Republic: Americans and their Politics in the Nineteenth Century, (Princeton: Princeton University Press, 2000).

[Ac07] 2007 Annual Report, ACCURATE: A Center for Correct Usable Reliable Auditable and Transparent Elections, 21 January 2008, http://accurate-voting.org/wp content/uploads/2008/01/2007.annual.report.pdf

[BB06] Dr. Nadja Braun, Daniel Brändli, Swiss E-Voting Pilot Projects: Evaluation, Analysis and How to Proceed, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).

[Bo06] Carol Boughton, Maintaining Democratic Values in e-Voting with eVACS®, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).

[Ca02] Jimmy Carter, Gerald R. Ford, Lloyd N. Cutler, Robert H. Michel, To Assure Pride and Confidence in the Electoral Process, Report of the National Commission on Federal Election Reform, (Brookings Institution Press, Washington, D.C., 2002).

[Ca05] Tracy Campbell, Deliver the Vote: a History of Election Fraud, an American Political Tradition – 1724-2004 (New York: Carroll & Graf, 2005).

[Ce04] Commission on Electronic Voting, "Interim Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System", March 2006.

[Cr04] Ann N. Crigler, Marion R. Just, Edward J. McCaffery, Rethinking the Vote: The Politics and Prospects of American Election Reform, (Oxford University Press, 2004).

[Ea07] United States Election Assistance Commission, EAC Receives Lab Recommendations from NIST, (Press Release 18 January 2007). http://www.eac.gov/ News/press/docs/01-18-07-eac-receives-lab-recommendations-from-nist

[GH07] Rop Gonggrijp and Willem-Jan Hengeveld "Studying the Nedap/Groenendaal ES3B voting computer a computer security perspective" 2007 USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, USA.

[Ha02] Help America Vote Act of 2002, United States Public Law 107-252, 107th Congress, http://www.fec.gov/hava/law_ext.txt

[MC03] Lorraine C. Minnite, David Callahan, Securing the Vote: An Analysis of Election Fraud, (New York: Demos, A Network for Ideas and Action, 2003).

[MM05] Ülle Madise, Tarvi Martens, E-Voting in Estonia 2005: The First Practice of Country-Wide Binding Internet Voting in the World, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).

[Ne07] Intrekking Regeling voorwaarden en goedkeuring stemmachines 1997, Uit: Staatscourant 19 oktober 2007, nr. 203 / page 10.

[So03] Office of the Secretary of State of California, Secretary of State Debra Bowen Moves to Strengthen Voter Confidence in Election Security Following Top-to-Bottom Review of Voting Systems, (Press Release 3 August 2003). http:// sos.ca.gov/ elections/ voting_systems/ttbr/db07_042_ttbr_system_decisions_release.pdf

[Tg07] Technical Guidelines Development Committee, Voluntary Voting System Guidelines, Draft, (United States Election Assistance Commission, 09/06/2007).

Session 5: Verification of E-Voting

Simple and Secure Electronic Voting with Prêt à Voter

David Lundin

University of Surrey, Guildford, Surrey, UK
d.lundin@surrey.ac.uk

Abstract: Prêt à Voter is an electronic voting system with very high security properties. We aim to make the system truly usable and applicable in elections with many races and candidates by allowing the vote to be formed using a voting machine and by printing a minimalistic receipt. We also introduce the procedure/technology mix concept to describe the use of procedures, people and technology to secure electronic voting systems.

1 Introduction

Implementing Prêt à Voter as it is described in a series of papers [Rya05, CRS05, RP05, RP06a, RS06a, Rya07b, LTR+06a, LTR+06b, XSH+07, LR08] has an associated set of fairly hard problems not envisaged by the authors, such as reliable optical character recognition (OCR), multi-page ballot forms in elections where there are many candidates contending many different races, chain of custody issues relating to pre-printed ballot forms, key distribution problems relating to on-demand printed ballot forms, and so forth.

Anecdotal evidence suggests that politicians and civil servants, in Europe and perhaps around the world, are concerned with the accessibility and applicability of electronic voting systems to a higher degree and cutting-edge security technology to a lesser degree than seemingly realised by researchers in the electronic voting field. Consider, for example, the impossibility for a civil servant in a country in continental Europe where there may, for example, be 28 candidates in each of seven races contended on the same ballot form to implement Prêt à Voter 2005 or 2006— the ballot form is simply too large to be scanned.

Further, anecdotal evidence suggests that a major contributor to decisions to use electronic voting in Europe is to simplify the process. For example, when the City of Hamburg, Germany, changed its electoral law it almost became a necessity to use some form of electronic counting of the votes as this would take days and weeks to do by hand [VV06]. The decision was taken to implement a completely new system based on Anoto pens and although this system was very accessible and had some procedures to safeguard the accuracy of the election, it seems it lacked sufficient technical guarantees.

This paper proposes a configuration of the Prêt à Voter electronic voting system in its later guises with emphasis on usability, accessibility and simplicity. Due to limitations to the length of this paper it has been necessary to leave out some technical detail but references provide this detail where necessary.

2 Preliminaries

In this section we describe the properties of end-to-end verifiable systems and introduce the procedure/technology concept.

2.1 End-to-End Verifiability

The will to elect leaders and representatives stems from a mass of people, equal, who have organised and created states and institutions to serve the population. From this philosophical point of view, some may say that once leaders were first democratically elected, they created election authorities and thus these are trustworthy and able to run fair elections for the people. Others are more reluctant to place such trust with such authorities. Consider, for example, some of those states in the world today that wish to disguise an undemocratic rule by holding unfair general elections . The most effective weapon against this at the disposal of the world's truly democratic nations is election observation.

However, election observation is a very blunt instrument with tremendous organisational and budgetary requirements. Although essential, election observation can only function as an audit of the procedures in place to safeguard the election and it is impossible to know, or prove, that the audit is sufficiently complete to allow conclusions to be drawn about the secrecy and fairness of the election.

This suggests that it would be more beneficial, if possible, to audit the election as a whole rather than some subset of the procedures involved. The ability to audit the whole election and (perhaps mathematically) prove that the outcome is exactly as indicated by the voters on election day has been given the name end-to-end verifiability and there exist many systems aiming to do this [AR06, ABBD04, ACvdG07, BFP+01, BT94, Cha04, CRS05, CGS97, FCS06, FOO92, JCJ05, LBD+03, NA03, OMA+99, Pun, Riv06]. There may be other ways of achieving this but we consider end-to-end verifiability a combination of two other: *voter verifiability* and *public verifiability*.

Voter verifiability The voter is given a receipt which she can use to check after the close of the election that her vote has been included in the tally. In order for the system to be coercion resistant, the receipt must not reveal the vote.

Public verifiability Any interested person or organisation can, perhaps using software, check that all the encrypted receipts are properly decrypted into plain text votes and that these are tallied correctly.

2.2 The Procedure/Technology Mix

We confess that we would rather employ a technological solution to security issues in electronic voting systems than a procedural one, but here feel obliged to introduce the *procedure/technology mix*. This is simply the mix of technology, procedures and people that constitutes any electronic voting system.

In the previous section, we claimed that the use of end-to-end verifiability would render the auditing of procedures and people obsolete. This is certainly true regarding the correctness of the outcome of the election; it is simply possible to prove whether the reported outcome is correct or not and if not, find the source of the error.

However, the *secrecy* of the election is, of course, a kind of property that once leaked cannot be "proven" back to secrecy. Furthermore, end-to-end verifiability is unfortunately very hard to achieve with technology only. Consider, for example, a theoretical system, the accuracy and secrecy of which depends on each voting device having its own secret private key. The distribution of these keys is, in fact, a procedural solution to both the accuracy and secrecy problems!

It therefore seems logical that the secrecy of the election is safeguarded by some mix of technology and procedures and we advocate a use of procedures to increase the accessibility of the system where a technological solution would reduce it.

3 Simpler Prêt `a Voter

3.1 Motivation

Our work with the first Prêt à Voter implementation and the subsequent demonstrations have resulted in the identification of two main problems impeding the progress toward the running of a general election:

1. *OCR*. The Optical Character Recognition (*OCR*) used in the first version of the system was not very robust and in order to interpret the marks as successfully as possible, it required the voter to use a seven segment display (like those you see in *LED* clocks) and a thick pen. Although all agreed that the success rate of the *OCR* can be increased, there was strong opposition from those with particular experience of implementing voting schemes against the seven segment display. It was felt that these were too cumbersome and hard to understand. We realise that this is not acceptable in a general election as such a voting system is used rarely by voters and this would introduce a large proportion of errors.

2. *Scanning*. The sheet-feed scanning of the ballot form is evidently very hard to use in elections where there are a number of races and/or a large number of candidates — election law may also stipulate that all races and candidates are printed on a single sheet, making this sheet immensely large. Furthermore, the layout of the ballot form would require that all candidates and their "boxes" were printed along the vertical axis of the paper, further limiting the number of races and candidates that can be printed on any piece of paper. Unfortunately, although that version of the Prˆet `a Voter implementation did support many concurrent different ballot forms, it did not support the spanning of a single race over more than one ballot form.

The motivation for this configuration of Prêt à Voter is thus simplicity, accessibility and the accommodation of a very large number of candidates. This introduces some procedural safeguards where technological safeguards have previously been envisaged [RS06b, Rya07b]. We argue that this is not only necessary but that it is so important to include as many voters and introduce as few errors as possible in the voting process, and that the procedure/technology mix must be adjusted.

3.2 The Voting Ceremony

In the polling station there are a certain number of voting machines placed in voting booths. The secrecy of the election is based on these voting booths providing proper privacy to the voter and the voting machine similarly being unable to leak the intention of the voter. Thus, there are poll station workers and guards keeping the area under surveillance in order to ensure that the machines cannot be tampered with.[32]

The voter is able to enter the polling station without first identifying herself to the poll station staff and she can enter a voting booth so as to interact with the voting machine. It is important that she not be required to identify herself before she can interact with the machine because this makes it harder for the poll station staff or machine to connect the will expressed in the interaction with the machine to a particular voter.

The main purpose of the voting machine is to help the voter express her will in the election, the difficulty of which depends on the election system in place and the abilities of the voter. As the voter is interacting with a computer to make her choices, the accessibility of the system is in itself an important area of research. It thus serves little use to go further into the details of how the voter interacts with the system to indicate her choices and it is sufficient to say that she may do so using her sight, touch and/or hearing and a touch screen, mouse, voice or other input device(s). At the end of the interaction the voting machine prints a vote in plain text (see Section 4.4) which the voter takes away and casts.

[32] Note that the accuracy is not threatened by this leak of information: but the privacy of the election is.

Interacting with the machine in the voting booth, the voter is able to produce some maximum number of votes. This must be a number greater than one so that the voter is able to create one vote that correctly captures her intention and some number of other votes that she can choose to audit, see below. The voting machine does not, therefore, know whether a vote it helps to construct will be audited or if it will be cast. It should therefore be disinclined to cheat (or malfunction) because there is some likelihood that it will be found out and taken out of commission. In order to stop voters from occupying voting booths too long and thus stopping others from voting, election law may stipulate some maximum number of votes, such as five or ten, which would be quite sufficient for the purpose.

When the receipt is printed by the machine, the voter can read it through and ensure that it is the vote she indicated to the machine. She turns the vote she is going to cast into an encrypted receipt (see below). Any or all of the other votes she may have created she is able to have audited by approaching an auditing desk. The barcodes on these ballot forms are scanned in by poll station workers and the forms are decrypted and the information printed. The voter is now able to check that the printed information does correspond to the vote she has just audited, indicating this vote was correctly formed. If so, she will grow more confident that the vote she will submit is also correctly formed.

Finally, the voter approaches a submission desk with the encrypted receipt she wishes to submit. She identifies herself to poll station workers and the barcode on the encrypted receipt is scanned and the contents of it are electronically submitted to a central repository (and may be noted next to the name of the voter who has cast it). Note that no submitted data need be kept secret to safeguard the secrecy of the election; it is already encrypted. After the close of the election, this, and all other encrypted receipts, will be decrypted as described in Section 4.7. A stamp is placed on the encrypted receipt by officials, indicating it has been submitted.

The voter can now leave the poll station with her encrypted receipt, and after the close of the election she can use a website to check for the inclusion of her vote in the tally. She does this by entering the serial number of her encrypted receipt and comparing the image of the receipt served by the website with the actual receipt. If the marks on these match exactly she can be confident that her vote is included in the tally.

4 Technical Foundation

4.1 Coping with Single Transferable Vote

In order to support Single Transferable Vote (STV) [Wik07, Soc07] and other schemes where the voter expresses a ranking or awards votes to more than one candidate, we employ the multiple-onion approach introduced by [Hea07]. We provide an overview of the scheme here.

A numerical representation of a candidate is encrypted under a probabilistic threshold public key cryptography scheme. There are many different such encryptions for each candidate and as these are encrypted under a probabilistic scheme they do not look alike. We call these encryptions onions. A set of onions are associated with each ballot form and the voter's choices, as expressed on the ballot form, are translated into an ordering of these onions. If the voter wishes to cast a vote for the candidates in the order C, E, A, D, B then this is encoded by ordering the constituent onions thus:

$O_C;O_E;O_A;O_D;O_B;O_{stop}$

Note that these are encryptions and which candidate they represent is therefore hidden. The stop onion O_{stop} is used to ensure that the length of the vote is not dependent on the number of choices expressed by the voter. A vote only for candidate C, for example, is thus constituted by an onion O_C,, the stop onion, and thereafter all other onions in a random order:

$O_C;O_{stop};O_A;O_E;O_D;O_B$

After the close of the election, the first constituent onion of each cast vote is decrypted and the vote given to the indicated candidate. This initiates the applicable STV protocol, which removes candidates and redistributes the votes according to the next choice in order in a number of rounds until the required number of candidates has been elected. Each time the vote is redistributed the next choice is decrypted. In our example, the first candidate is decrypted thus:

$C;O_E;O_A;O_D;O_B;O_{stop}$

If candidate C is subsequently eliminated and his or her votes redistributed, the onion representing candidate C is appended, the plaintext representation of C removed and the next onion decrypted, thus:

$E;O_A;O_D;O_B;O_{stop};O_C$

This is now a vote for E. When a decryption reveals the stop onion, the vote is removed from further redistributions. Each redistribution round contains a re-encryption shuffle so as to hide the ordering of the candidates in the vote; please see [Hea07] for details. This configuration thus limits the impact of an attack popularly called the Italian attack [Hea07] where the ordering of the candidates carries some message to a coercer.

4.2 Pre-Creation of Onions

A source of potential threats to the secrecy of the election pointed out in early papers describing end-to-end verifiable systems [Rya05, BR03, RP05, KSW05, RP06a, RS06a, RP06b, Rya06, Rya07a] was that the voting machine must select random values and errors or predictability in the pseudo-random number generator may render the cryptography useless. Furthermore, the voting machine might use "random" values from a list shared with a culprit or values such that a hash thereof would signal to a culprit the contents of the vote and/or the identity of the voter. To remove this problem, we do not require the machine to select the randomness used in creating the candidate list but employ the distributed pre-creation technique detailed in [RS06a].

4.3 Touch Screen Interface

To accommodate for elections with many races and/or races with many candidates, the proposed configuration of Prêt à Voter has two major differences to previous versions: (a) the receipt is created by a voting machine and (b) the receipt is printed in the *minimal* form presented in the next section.

4.3.1 Creating a Vote with the Machine

This is an example of a possible interaction with the voting machine. The steps involved can be different in appearance, order and number and are adapted to the election. Approaching an idle voting machine, the voter is greeted with a message asking her to touch the screen to initiate the voting process.

Springfield Local Election Tap screen to start

A list of races is shown with indicators to whether or not a vote has been created in each race. The voter selects a race by tapping the screen[33].

Select race	
Mayor	Not voted
Sanitation Commissioner	Not voted

A list of the candidates in the selected race is shown and the voter is able to tap a single candidate or a number of candidates in the preferred order. A "Clear" button is available on the screen, which clears all choices made and allows the voter to start over. A "Proceed" button allows the voter to return to the list of races.

[33] Or using some other input method, depending on the abilities of the voter.

Vote for Sanitation Commissioner	
Shmoikel Krusotsky Apu Nahasapeemapetilon Ray Patterson Homer Simpson	

Selecting her favourite candidate, the voter completes the vote for the race and clicks the "Proceed" button to return to the race selection screen.

Select Race	
Mayor Sanitation Commissioner	Not Voted Voted

The voter is able to return to any race and re-create her vote. A "Proceed" button on the race selection screen allows her to go to a summary screen. Here the voter can select either of two buttons: "Go back" or "Print vote".

Summary of your vote	
Mayor Sanitation Commissioner	Not voted Homer Simpson

When the voter is finished and presses the "Print vote" button, the machine displays a final message whilst printing the vote.

Thank you Please take your printed vote

4.4 The Minimalistic Encrypted Receipt

The purpose of the minimalistic encrypted receipt is to enable the printing of many races on the same receipt and to aid the voter in checking the receipt on the web bulletin board. To achieve this we wish to print as few candidates as possible on the vote. We first introduce the traditional Prêt à Voter ballot form and its associated encrypted receipt before showing the alterations we propose to these.

4.4.1 The Prêt à Voter Ballot Form and Encrypted Receipt

The ballot form in Prêt à Voter consists of two columns: in the left the candidates are printed in a random order (based on randomness unique for the form) and in the right the voter makes her marks in a grid corresponding to the candidates in the left column. For example:

Ballot form	
Sanitation Commissioner	
Homer Simpson	
STOP	
Apu Nahasapeemaptelon	
Ray Patterson	
Smoikel Krustofsky	
	lk3j92784

If a voter makes her marks in the right hand side grid and then detaches and destroys the left hand column, the remaining encrypted receipt does not reveal her vote. However, a value called the onion, printed at the bottom of the grid, can be decrypted to reveal the vote. In this example an encrypted receipt may be:

2
3
1
lk3j92784

It has been envisaged that the Prêt à Voter is a single page, which contains all races in the election and all the candidates in each of those races. The voter makes her mark on the paper and detaches and destroys half, producing an encrypted receipt which is subsequently scanned and then handled electronically. It is quite clear that in an election with many races and many candidates, it is not possible to print all on one piece of paper that can also be fed through a scanner after the marks have been made by the voter.

4.4.2 The Minimalistic Encrypted Receipt

The traditional Prêt à Voter ballot form is printed onto paper before the election (or on demand before they are used [RS06a, LR08]) and as the voter uses a pen to fill out her choices, naturally all candidates must be available on the ballot form. In the scheme presented here a computer is used to create the vote after which the ballot form is printed. Therefore, it is possible to print only the candidate(s) that the voter has indicated a vote for. In our example, when the voter makes her marks using the touch screen she may indicate her choices thus (note that the candidates are listed in the alphabetical order on the screen):

Vote for Sanitation Commisioner	
Shmoikel Krustofsky	
Apu	
Nahasapeemapetilon	
Ray Patterson	1
Homer Simpson	2

When the voter presses the "Print receipt" button the voting machine retrieves the necessary onions and decrypts these (see above) to find the ordering of the candidates. Let us assume in our example that the machine retrieves the onions with serial number 27344, decrypts these and finds that the candidate list has the following order:

27344
Homer Simpson
STOP
Apu
Nahasapeemapetilon
Ray Patterson
Shmoikel Krustofsky

The machine now prints the following filled-out Prêt à Voter ballot form, note that only the candidates which the voter has indicated are printed and that these are printed in the order dictated by the onions:

Ballot form	
Sanitation Commissioner	
Homer Simpson	2
STOP	3
Ray Patterson	1
	1,2,4 27344

In this example we are only able to avoid printing two candidates, but in a race with many more candidates the same number of choices made by the voter would drastically reduce the number of candidates that must be printed. The index numbers 1; 2; 4 of the candidates printed are displayed at the bottom right together with the serial number 27344. These values can be printed in the form of a barcode (see below) which allows them to be read in quickly. Note that these numbers together with the choices indicated above by the voter is all that is needed to represent the vote. The voter now checks that the printed vote is truly a representation of her intended vote. If it is not she can discard the vote (by shredding it for example) and produce another. If she is happy with the vote and wishes to cast it, she detaches the two columns from each other and destroys the left hand one. What remains is an encrypted receipt:

2
3
1
1,2,4 27344

The voter approaches a desk manned by poll station staff, identifies herself and allows the barcode on the encrypted receipt to be scanned. When poll station staff are satisfied that the barcode has been scanned and electronically transmitted to the web bulletin board they stamp the encrypted receipt with an official stamp so as to indicate that it is the receipt of a vote that has been cast in the election. A mark is placed in the register to indicate that this voter has cast her vote[34]. All votes submitted in this way are collected on the web bulletin board.

4.4.3 The Barcode

All previous versions of Prêt à Voter has required an encrypted receipt to be scanned in and interpreted to form a digital representation that could subsequently be decrypted. This OCR process has been shown to be a significant weakness to the scheme: it results in many errors[35].

In this scheme we reduce the amount of work in the scanning process to the recognition of a barcode. These are printed in such a way as to be simple to read and recognise and they can contain check numbers etc to aid the correct interpretation of them. In order to record a vote the system must read the following information from the encrypted receipt:

[34] In some constituencies, such as the United Kingdom, the law requires that the ballot form serial number is noted against the name of the voter: that is quite possible to do in this scheme.
[35] Note that these errors did not mean that a vote was cast for a different candidate than indicated by the voter —but that the vote had to fill out another ballot form as the first could not be correctly understood by the system.

1. The serial number (27344)

2. Which candidates are shown on the ballot form (1; 2; 4)

3. The marks made by the voter (2; 3; 1)

To enter this information into the barcode, we simply concatenate them:

27344|1; 2; 4|2; 3; 1

When this information is scanned by poll station staff it is submitted to the web bulletin board. Here the appropriate constituent onions are retrieved:

27344
$O_{RSimpson}$ O_{RSTOP} $O_{RNahasapeemapetilon}$ $O_{RPatterson}$ $O_{RKrustofsky}$

The appropriate onions are selected (numbers 1, 2 and 4 in our example) and re-ordered in the correct order as indicated by the choices (2, 3 and 1) — thus the onions are placed in the following order:

27344
$O_{RPatterson}$ $O_{RSimpson}$ O_{RSTOP}

Note that of course the contents of these onions are unknown! Therefore, the system now holds an encrypted vote submitted by this voter.

4.5 Auditing a Vote

We here argue that it is safe to allow a voter to use a voting machine to create the vote, because she may create any number of votes and audit some of these. If the voting machine attempts to cheat, it cannot be sure that the vote will not be audited and its cheating thus found out. A malfunctioning machine will thus be found with a high probability and taken out of commission.

The first audit that a voter makes out of a vote printed by the voting machine is simply to read it. If the machine has committed an error (or something worse) then the marks printed would not match the intention of the voter. If this is the case, she can simply destroy the vote and create another one — until she receives one that correctly indicates the vote she wishes to cast. Note that the voter may have performed some "human" error while interacting with the machine and not spotted this until the vote has been printed: this gives her another chance to spot such a mistake and to rectify it.

The second audit of the ballot form that can be performed on any vote is the checking of the barcode. This is simply done by the voter allowing the barcode to be scanned by a machine available in the polling station, which shows the contents of the barcode in a human readable form. Such machines can also be supplied by independent organisations — or run as a small piece of software on the voter's camera-enabled mobile phone. The voter then simply checks that the information shown by the reader corresponds to the information printed in the right column of her vote.

Finally, if the voter decides to audit a created vote then the constituent onions shall be retrieved from the web bulletin board (where they are marked as audited, ensuring that no vote can subsequently be cast with these onions) and decrypted by the tellers. The full candidate list is then displayed to the voter who compares it to the printed vote.

The purpose of this audit is first to find any machine that may malfunction or that has been compromised. Secondly, the audit functions to convince voters that the system is working correctly and that the vote will be decrypted correctly.

4.6 Checking the Receipt

The voter is allowed to take home the scanned and stamped encrypted receipt. She can then, at any time, visit the web bulletin board on the web and search for the serial number printed on the receipt. When she calls up her receipt she should see an exact replica of the receipt she holds in her hands. If this is the case then the voter can be certain that her vote has been included in the final tally. If the receipt is not found on the web bulletin board or if the version she finds there does not match the one she has in her hand, she can accuse those in charge of running the election of malfunction or fraud and she has proof in her receipt that she has cast a vote which is now missing or has been changed.

4.7 Decryption and Tallying

At this stage the web bulletin board contains a list of all encrypted votes that have been cast, in the form of a number of ordered onions. We are unable to describe the decryption here because of limitations to the length of this paper but a detailed specification is available in [Hea07].

4.8 Note on Securing the Machine using Procedures

It is important to note that the accuracy of the election, that is to say, the trustworthiness of the outcome of the election, is safeguarded not by procedures but by the cryptographic properties of the system. The result of the election is thus as trustworthy as in previous configurations of Prêt à Voter [CRS05, RS06a], because they all rely on the same verifiability.

5 Discussion

The main advantages of the proposed scheme is that the voting machine is able to guide the voter through a potentially very complex voting procedure involving any number of races and any number of candidates in those races. The voter turns the plain text vote into an encrypted receipt and the scanning of this receipt is very fast because only a barcode has to be scanned. The main disadvantage to this configuration of Prêt à Voter is that the voting machine must learn the voter's intention in order to produce the printed vote. The secrecy of the election is thus safeguarded simply by procedures that ensure that the machine does not leak any information. As discussed in the introductory sections of this paper, there is a necessity to alter the procedure/technology mix so that it is possible to make the system more accessible and remove a large proportion of the errors associated with the filling out of the ballot form.

5.1 Acknowledgements

Thanks to the anonymous EVOTE08 reviewers for their feedback. Thanks also to Peter Ryan, Steve Schneider, James Heather, Roger Peel, Zhe Xia, Kieran Leech, Roberto Araújo and Jacques Traore, who listened to a presentation of initial ideas.

References

[ABBD04] R. Aditya, Lee B, C. Boyd, and E. Dawson. An efficient mixnet-based voting scheme providing receipt-freeness. Proceedings of TrustBus'04, pages 152–161, 2004. LNCS 3184.

[ACvdG07] Roberto Araujo, Ricardo Filipe Custodio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel. Proceedings of Workshop On Trustworthy Elections (WOTE 2007), 2007.

[AR06] B. Adida and R. Rivest. Scratch & Vote: self-contained paper-based cryptographic voting. Proceedings of the fifth ACM workshop on Privacy in electronic society, pages 29–40, 2006.

[BFP+01] O. Baudron, P.-A. Fouque, D. Pointcheval, J. Stern, and G. Poupard. Practical multicandidate election system. Proceedings of the twentieth ACM Symposium on Principles of Distributed Computing (PODC'01), pages 274–283, 2001.

[BR03] J. Bryans and P. Y. A. Ryan. A Dependability Analysis of the Chaum Digital Voting Scheme. Technical Report, University of Newcastle, CS-TR:809, 2003.

[BT94] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections (extended abstract). Proceedings of the twenty-sixth Symposium on Theory of Computing (STOC'94), pages 544–553, 1994.

[CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multiauthority election scheme. Advances of Eurocrypt'97, pages 103–118, 1997. LNCS 1233.

[Cha04] D. Chaum. Secret ballot receipts: true voter-verifiable elections. IEEE: Security and Privacy Magazine, 2(1):38–47, 2004.

[CRS05] D. Chaum, P. Y. A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. Proceedings of the tenth European Symposium on Research in Computer Science (ESORICS'05), pages 118–139, 2005. LNCS 3679.

[FCS06] K. Fisher, R. Carback, and T. Sherman. Punchscan: Introduction and System Definition of a High-Integrity Election System. In PRE-PROCEEDINGS, pages 19 – 29. IAVoSS Workshop On Trustworthy Elections, 2006.

[FOO92] A. Fujioka, T. Okamoto, and K. Ohta. A Practical Secret Voting Scheme for Large Scale Elections. Advances of Auscrypt'92, pages 244–251, 1992. LNCS 718.

[Hea07] J. Heather. Implementing STV securely in Prêt à Voter. 20th IEEE Computer Security Foundations Symposium (CSF'07), pages 157–169, 2007.

[JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. Proceedings of the 2005 ACMWorkshop on Privacy in the Electronic Society, pages 61–70, 2005.

[KSW05] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: a systems perspective. Proceeding of USENIX Security Symposium, pages 186–200, 2005. LNCS 3444.

[LBD+03] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. Proceedings of ICISC'03, pages 245–258, 2003. LNCS 2971.

[LR08] D. Lundin and P. Y. A. Ryan. Human readable paper verification of Prˆet `a Voter. Technical Report at the University of Surrey, CS-08-03, 2008.

[LTR+06a] D. Lundin, H. Treharne, P. Y. A. Ryan, S. Schneider, and J. Heather. Distributed creation of the ballot form in Prêt à Voter using an element of visual encryption. Proceedings of Workshop On Trustworthy Elections (WOTE 2006), pages 119–125, 2006.

[LTR+06b] D. Lundin, H. Treharne, P. Y. A. Ryan, S. Schneider, J. Heather, and Z. Xia. Tear and destroy: chain voting and destruction problems shared by Prˆet `a Voter and Punch- Scan and a solution using visual encryption. Proceedings of Workshop on Frontiers in Electronic Elections (FEE 2006), 2006.

[NA03] C. A. Neff and J. Adler. Verifiable e-voting: indisputable electronic elections at polling places. VoteHere Inc, 2003.

[OMA+99] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. Information Security'99, pages 225–234, 1999. LNCS 1729.

[Pun] Punchscan. http://www.punchscan.org.

[Riv06] R. Rivest. The ThreeBallot voting system, 2006. http://crypto.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf.

[RP05] P. Y. A. Ryan and T. Peacock. Prêt à Voter: a system perspective. Technical Report of University of Newcastle, CS-TR:929, 2005.

[RP06a] P. Y. A. Ryan and T. Peacock. Putting the human back in voting protocols. Technical Report of University of Newcastle, CS-TR:972, 2006.

[RP06b] P. Y. A. Ryan and T. Peacock. Threat analysis of cryptographic election schemes. Technical Report of University of Newcastle, CS-TR:971, 2006.

[RS06a] P. Y. A. Ryan and S. Schneider. Prêt à Voter with re-encryption mixes. Proceedings of ESORICS, 2006. LNCS.

[RS06b] P. Y. A. Ryan and S. Schneider. Prêt à Voter with re-encryption mixes. Technical Report of University of Newcastle, CS-TR:956, 2006.

[Rya05] P. Y. A. Ryan. A variant of the Chaum voter-verifiable scheme. Proceedings of the 2005 Workshop on Issues in the Theory of Security, pages 81–88, 2005.

[Rya06] P. Y. A. Ryan. Verified encrypted paper audit trails. Technical Report of University of Newcastle, CS-TR:966, June 2006.

[Rya07a] P. Y. A. Ryan. The computer ate my vote. Technical Report of University of Newcastle, CS-TR:988, 2007.

[Rya07b] P. Y. A. Ryan. Prêt à Voter with Paillier Encryption. Technical Report of University of Newcastle, CS-TR:1014, 2007.

[Soc07] Electoral Reform Society. 2007. http://www.electoral-reform.org.uk/.

[VV06] M. Volkamer and R. Vogt. New Generation of Voting Machines in Germany — The Hamburg Way to Verify Correctness. In PRE-PROCEEDINGS, Hamburg, Germany, 2006. Frontiers of Electronic Elections (FEE 2006).

[Wik07] Wikipedia. Single transferable vote, 2007. http://en.wikipedia.org/wiki/Single transferable vote.

[XSH+07] Z. Xia, S. Schneider, J. Heather, P. Y. A. Ryan, D. Lundin, R. Peel, , and P. Howard. Prêt à Voter: all in one. Proceedings of Workshop On Trustworthy Elections (WOTE 2007), 2007.

Improving the Farnel Voting Scheme

Roberto Araújo[1], Peter Y. A. Ryan[2]

[1]Department of Computer Science, TU-Darmstadt
Hochschulstrasse 10, D-64289 Darmstadt, Germany
rsa@cdc.informatik.tu-darmstadt.de

[2]Centre for Software Reliability, Newcastle University
Newcastle upon Tyne NE1 7RU UK
peter.ryan@ncl.ac.uk

Abstract: Farnel is a voting scheme which first introduced the concept of a ballot box to exchange votes. Recently, Araújo et al. improved this concept to accomplish a voter-verifiable scheme in which voters receive copies of receipts of one or more randomly selected previous cast votes. The scheme, however, relies on a strong requisite to achieve security: trustworthy talliers. With the goal of removing this requisite, in this paper we propose a Prêt-à-Voter style receipt for this scheme. In addition, we present a novel way to initialize the Farnel box and a new scheme based on combining Farnel with Prêt-à-Voter style encoding of receipts.

1 Introduction

Voter-verifiability is a novel security feature provided by several recent voting systems, such as Prêt-à-Voter [Rya04, CRS05] and Punch Scan [PH06]. It allows voters to verify that their votes are accurately counted by means of *protected receipts* and so gives more confidence to the election process. The voters, however, cannot use their receipts to compromise their privacy, even if they are prepared to cooperate with the coercer.

High-assurance voting systems typically rely on cryptography to achieve security and to implement voter-verifiability. Such technology makes the security of modern systems comparable or even better than traditional paper-based elections. However, systems that employ cryptography are not easily grasped by the average voter and so voters need to rely on the assurances of experts.

With the goal of making such schemes more understandable, Randell-Ryan [RR06], Rivest [Riv06, RS07], and Araújo et al. [ACvdG07], introduced voter-verifiable schemes that do not rely on cryptography. These schemes are simple and can be more easily understood by the voters. However, they do not achieve the same levels of assurance as the cryptographic systems. In the scheme proposed in [Riv06], the ballot secrecy is not perfect and it may reveal statistical indications of voting results before the voting end. The proposals of Araújo et al. and of Randell-Ryan require trustworthy talliers or additional mechanisms to counter threats during the vote tabulation.

In this paper we introduce improvements for the scheme of Araújo et al. Especially, we propose a Prêt-à-Voter style receipt in order to detect manipulation of votes by adversaries, including malicious talliers. In addition, we present a novel way to initialize the Farnel box and a new scheme based on combining Farnel [ACvdG07, Cus01] with Prêt-à-Voter style encoding of receipts. Our proposals make use of cryptography to overcome the drawbacks of the previous non-cryptographic solutions.

This paper is organized as follows: in the next section we describe the elements of the Farnel mechanism. In Section 3 we introduce a new ballot form for the scheme of Araújo et al. Then, in Section 4, we show a new scheme based on Farnel that employs only one ballot box. Finally, we present our conclusions in Section 5.

2 Preliminaries

We present here the basic elements of the Farnel approach. The Farnel type voting schemes [ACvdG07, Cus01] are based on the observation that to achieve voter-verifiable it is not necessary for the voter to carry away a receipt corresponding to their own vote. The Farnel approach then is to provide voters, when they cast their votes, with copies of receipts of one or more randomly selected previous cast votes.

This idea has a number of attractive features: ballot secrecy is achieved up front and does not have to be provided by anonymising mixes, etc. during tabulation. In fact, plaintext receipts can be used in contrast to the encrypted receipts of many other voter-verifiable schemes, e.g. [Rya04]. Furthermore, any fears that voters might have that their vote is not truly concealed in an encrypted receipt is mitigated. The Farnel mechanism also mitigates randomization style attacks.

2.1 The Farnel Ballot Box

The Farnel is a concept of ballot box that was first introduced by Custódio [Cus01]. This ballot box performs differently from a conventional one. It is able to shuffle its contents and is initialized with elements (e.g. votes). After receiving elements from voters, it returns to them elements that correspond to randomly selected, previously cast votes. Recently, Araújo et al. [ACvdG07] improved the Farnel concept in order to accomplish a voter-verifiable scheme. In the improved concept, besides shuffling its elements, the Farnel box should be able to copy some elements and to remove scratched surfaces.

We describe the enhanced Farnel box as follows: it is a box that has mechanisms to remove scratch surfaces, and to shuffle and to copy elements in a memoryless way. The box has an initial set of elements cast before the voting. At the time of voting, it is able to receive an element, to shuffle its contents, to copy one or more randomly selected elements from its set, to output the copies, and to add the element received to its set. The box elements may be votes or receipts.

Although the requisites of the Farnel box seem difficult to implement, a tombola (i.e. a raffle drum) normally used in lottery games to shuffle tickets could form the basis of an implementation of the box.

The Farnel box was never formally specified. This way, we introduce now a specification of the box in the process algebra CSP.

Let Init denote the initial set of dummy ballots (say votes or receipts) with which the box is initialized. Let l denote the number of receipts to be output to each voter when they cast their votes and ballots the set of all possible ballots. Then the Farnel box will start in state Farnel (Init) and its subsequent behavior is defined recursively as:

$$Farnel_l(X) := cast?\ b{:}Ballots \rightarrow \Box receipt!\ r{:}\wp_l(X) \rightarrow Farnel_l(X \cup \{b\})$$

We have used the notation Ãl(*X*) to denote set of subsets of *X* of cardinality *l*.

Thus, the Farnel ballot box is parametrised by the integer *l* and its initialization *Init*. At any point, the box can accept a ballot *b*, after which it outputs a set of ballots in size *l* chosen at random from its current set *X*. After this, the new ballot is added to *X* and the box is ready to receive the next ballot.

2.2 The Initialization Process

The initialization process takes place before the election and is performed by the authorities in a public session. The main objective is to cast a predefined number of votes (or receipts) into the Farnel ballot box and to publish the number of elements cast per option on the bulletin board.

The elements cast before the election are necessary mainly for ensuring the anonymity of the early voters. As the Farnel receives an input from each voter and outputs copies of random elements, it must have an initial set of elements to choose from. Otherwise, after receiving inputs, the Farnel would not have enough elements to select at random and to make the copies.

For the schemes that we describe here, it is necessary to ensure that ballots cast during the initialization are well formed in some way. This will typically involve some form of random auditing. Thus, for example, we might require that 2x blank ballots be created beforehand. The authorities perform the following steps to initialize the ballot box:

(1) Select x blank ballots at random and audit them as necessary. Ballots audited are discarded; (2) Mark the other x unaudited blank ballots according to the number of votes per option specified in advance; (3) Cast the x marked ballots (or receipts) into the Farnel box and publish the number of elements cast on the bulletin board.

Notice that in schemes which employ a conventional and a Farnel box (e.g. [ACvdG07]), the conventional box is initialized with votes and the Farnel is initialized with the corresponding receipts. Also, for schemes using plaintext ballots, the auditing for well-formedness is not necessary and would be omitted.

In order to prevent manipulation, the initialization process should be scrutinized by helper organizations. They should check that the ballot box is empty before it is initialized, as well as verify that all procedures above are performed correctly. Further, the ballot box should be sealed and continually supervised by third parties after the initialization. The seal is removed when the voting starts.

2.2.1 Initialization of the Farnel box with Void Ballots

Where we are using encrypted receipts we have an alternative way to initialize the Farnel box: we include a void option on the ballots and initialize the box with ballots representing votes for the void option. This has the advantage that we do not have to keep a log of the actual votes cast for each candidate during initialization. We do need a robust mechanism to ensure that all initializing votes are cast for void, but it seems likely that this is easier to enforce than maintaining a record of an initial tally. We can use this approach for the Prêt-à-Voter and ThreeBallot style ballots, but not where plaintext receipts are used.

2.3 The Parameters of the Farnel Box

The Farnel box is initialized with a number of elements (votes or receipts) before the voting starts and outputs copies of its elements during the voting, as described. The initial elements ensure the voter's anonymity while the copies are handed to the voter as her receipt. The number of initial elements, as well as the number of receipts given to each voter, compose the parameters of the box.

In order to preserve the voters' anonymity, the initial elements and the voters' elements cannot be distinguished through the copies output by the Farnel box. The number of initial elements is fundamental for guaranteeing this. As the Farnel box outputs elements for each voter, the elements of the early voters have more chance to be output. Hence, these elements may be distinguished from other elements. Depending on the number of initial elements, however, the chance of distinction may be negligible as the initial elements may also be output.

To achieve verifiability while maintaining anonymity, the number of initial elements and the number of receipts should be defined such that:

(1) The voter's anonymity is preserved even if the Farnel box is able to output a copy of her element; (2) An individual receipt or a set of them do not provide enough information to distinguish elements; (3) The number of copies of elements in all receipts is sufficient to detect accuracy problems with an acceptable probability (i.e. the probability that the corruption of any given vote is detected is at least 50%).

We require that the voter should not be able to obtain any information other than her choice when casting her element.

Taking into account these requisites, we have a number of possible strategies for initializing the box: ballots marked at random (with the totals carefully recorded), a predetermined number of votes per option, votes for a void option, or a combination of these methods. If we adopt an initialization with votes for void, we must include a minimal number of votes for the other options. Otherwise, the first voter may vote and receive a copy of her own vote as receipt. An initialization purely with void votes only works if we have mixes during the tabulation. This might seem like overkill since anonymity is already provided by the Farnel mechanism. However, it might still be useful in some contexts and does provide an extra layer of protection.

Note that in the specification of the Farnel box presented before, the box is not able to output the element it receives.

3 A New Ballot Design for the Farnel Variant Scheme

The Farnel scheme was proposed by Custódio [Cus01] (see [ACvdG07] for a description). The scheme employs an original Farnel ballot box and relies on physical signatures. However, it is not voter-verifiable. Recently, Araújo et al. [ACvdG07] introduced a variant of the Farnel scheme. In contrast to the original version, the scheme is voter-verifiable and does not employ signatures. It relies, though, on trustworthy talliers to tabulate the votes.

With the goal of removing this requisite, we introduce in this section a new ballot design for Araújo et al.'s proposal.

3.1 An Overview of Araújo et al.'s Farnel Variant Scheme

The scheme employs a ballot form composed of two halves that are linked by a unique ID and that are separated by perforations. More specifically, the ballot has an options half composed of the voting options as well as an ID and an ID half that contains the same ID of the options half (see Figure 1). These IDs are covered by scratch surfaces.

Figure 1: The ballot form of the Farnel variant scheme.

Besides the unusual ballot form, the scheme depends on two ballot boxes. One of them is conventional and the other is a Farnel box. These boxes are initialized before the voting. That is, the conventional box receives dummy votes (i.e. marked option halves) and the Farnel box receives the ID halves (i.e. receipts) corresponding to the votes. The scratch surfaces in the halves are detached during the initialization and at the end the number of votes cast is published on a bulletin board.

At time of voting, the voter receives a blank ballot and detaches its scratch surfaces. She then compares the IDs on the halves and if they match, she marks her option. After that, she separates the two halves of her ballot, casts the option half into the conventional box, and the other half into the Farnel box. Upon receiving the half, the Farnel box shuffles its ID halves and copies a set of them as receipt to the voter. As alternative to avoid comparison of IDs, the scheme may have an auditing process to check ballots before the voter receives her blank ballot and require the voter to cast her vote without removing the scratch surfaces. The Farnel box then removes the scratch of the half that it receives.

After the voting, the authorities publish the content of both ballot boxes on the bulletin board and count all votes from the conventional box. The dummy votes are then subtracted from the total of votes to obtain the results.

In order to verify the votes published on the bulletin board, voters and observers compare the ID halves with the IDs in the options halves. The voters can also match the IDs on their receipts with the options halves on the board.

3.1.1 Drawback

Due the receipt style employed, the proposal requires trustworthy talliers. These authorities should supervise the votes strictly after opening the ballot boxes. On the contrary, an adversary (e.g. a malicious tallier) is able to compromise the voting results as follows.

According to the scheme, the two halves of all ballots are published after the voting. This way, they can be compared to verify the exactness of the voting results. Before publishing the options halves, though, an adversary could replace a vote (i.e. a marked option half) by a new one marked to a different option, but that contains the same ID of the replaced vote. This substitution would not be detected by voters and observers, as they only compare IDs.

3.2 Combining the Farnel Variant Scheme and Prêt-à-Voter

The main problem of the receipt used in Farnel variant is that it does not depend on the option chosen. This way, an adversary is able to replace votes without being detected. In order to detect such a problem, a receipt should contain some information related to the option selected. However, this information should not reveal the option itself before the voting closes and should still be able to detect replacement of votes. Otherwise, the receipt can leak statistical information about the voting results as the Threeballot scheme [Riv06, RS07] (see [ACvdG07] for details). We introduce now a new ballot design for the Farnel variant that satisfies these requirements.

3.2.1 The Ballot Form

Our ballot form is based on the Prêt-à-Voter [Rya04, CRS05] ballot and is inspired by the ideas of Randell-Ryan [RR06] and of Scratch-and-vote [AR06]. Differently from the original Prêt-à-Voter ballot design, however, the ballot here does not include a mixnet onion.

The ballot is composed of two pages that are overlaid initially. The top page has a list of voting options in a random order with a selection bubble beside each option. The top page also includes a commitment to the list of options and its respective decommitment value. The bottom page contains the same bubbles and the same commitment as the top page. The commitment printed on both pages, as well as the value to open it on the top page, are covered by scratch surfaces. A carbon mechanism transfers the selections from the top page to the bottom page (see Figure 2 for an example of this ballot form).

Formally, the new ballot form is described as follows: Let C be a set of options available, π_C a permutation of C, H a secure hash function used here as commitment, and r a random number from a large (key) space. π_C, $H(\pi_C, r)$, r, and bubbles to select an option compose the top page. The bottom page contains *only* $H(\pi_C, r)$ and the bubbles in same position of the top page.

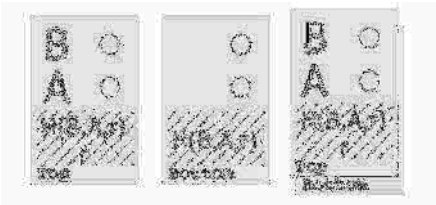


Figure 2: The proposed ballot form for the Farnel variant scheme.

The new ballot form satisfies the requisites above. The votes now are tabulated from the top pages and the receipts are made from the bottom pages (without the scratch surfaces). Because each bottom page contains the same selections of its corresponding top page and also includes the commitment to the options on the top page, an adversary cannot replace a top page by another with a different permutation or with a selection for a different option, without being detected. Moreover, since the bottom page does not include the option selected, an adversary cannot use receipts to obtain indication of the results before the voting closes.

3.2.2 New steps for the Initialization, the Voting, and the Tallying phases

Due the modification of the ballot form, the initialization, the voting and the tallying steps in the original scheme need to be adapted.

Before the Voting

The conventional box and the Farnel box are now initialized with marked top pages and with bottom pages, respectively (see also Section 2.2). Before initializing the boxes, however, the officials publicly audit ballots as follows: they separate the pages of each ballot and scratch off their surfaces; they then hash the options and the random number on top page, and compare the result with the hashes on both pages. Ballots audited are discarded.

Voting

In the voting phase, upon proving her eligibility to the voting authorities, the voter receives a sealed envelope with a blank ballot. If required by the voter, her ballot can be audited (as above) and she receives a new blank ballot. The voter performs the following steps to vote:

1. (Selecting the option) In the voting booth, the voter marks her choice on the top page and it is transferred to the bottom page.

2. (Verifying the ballot) She then inserts her ballot into a special envelope, which has transparent borders and a window to show just the scratch surface. After this, she hands the envelope to the authorities. They verify that the surface on the top page is intact and that the voter did not separate the two pages.

3. (Casting the top page) The voter separates the pages of the ballot and casts the top page into the conventional ballot box.

4. (Obtaining the receipt) She casts the bottom page into the Farnel box. The box shuffles its contents and outputs copies of randomly selected bottom pages as receipts.

Observe that the special envelope prevents the authorities to learn the voter's choice while verifying the surfaces, and the pages were not separated before.

Tallying and Verifying the Votes

As the Farnel variant scheme, the contents of the two ballot boxes are published on a bulletin board in the tallying phase. Now, the scratch surface on the top pages should be removed before publishing the ballots and the commitments should be decommited to verify the ballots. That is, the random number and the options on the top page are hashed together and the resulting hash is compared with the hash on both pages.

From the pages published on the bulletin board, everyone can perform the same procedures as the talliers to verify the votes. The voters, especially, match their receipts with the corresponding bottom pages on the board.

4 Single Box Farnel Scheme

The design presented above is awkward in several respects: it requires two ballots boxes and the vote casting procedure is rather complicated and vulnerable to certain threats. We present here an improved version of the Farnel variant that requires just one ballot box and uses a simpler vote casting procedure.

4.1 Requisites

The ballot form

As the design presented in Section 3.2.1, the ballot here is composed of two pages that are initially overlaid. The top page, though, contains *only* the options in a random order along with bubbles to select them. The bottom page contains the same bubbles as the top page and an index. Also, it includes one commitment to the options of the top page and the index. The index indicates the options' order and helps the authorities to identify the order in the tallying process. The commitment and the index are printed at the foot of the page, on the left and on the middle, respectively. In addition, the bottom page includes the corresponding decommitment that is printed close to the index. The commitment is covered by a scratch surface apart from the index and from the decommitment.

More formally, let C be a set of options available, I a set of positive integers, π_C a permutation of C, H a secure hash function used as commitment, i an index that is a unique number in I, and r a random number from a large (key) space. The top page is composed of π_C and bubbles to select the options. The bottom page contains $H(\pi_C, r, i)$, r, i, and the same bubbles of the top page (see also Figure 3).

The list of possible permutations (i.e. options' orders) for all ballots and the index corresponding to each permutation are published on the bulletin board before the voting.

The Ballot Box

The scheme employs just a Farnel ballot box that is initialized (see Section 2) with marked bottom pages before the voting starts; the corresponding top pages are destroyed.

4.2 The Scheme

Before the Voting

As required by the Farnel box, we define a number of copies l that each voter receives as receipts and initialize the box with a number of dummy votes (Section 2 details this process).

For the initialization as well as for the voting phase, we require an auditing process. The audit is necessary to detect malformed ballots and is performed as follows: the authorities select a set of ballots at random, separate the two pages of each ballot, and detach their scratch surfaces. In order to verify a ballot, the authorities hash the options on the top page along with the random number and the index printed on the bottom page. They then compare the resulting hash with the value H(pC,r,i) also on the bottom page. Moreover, the authorities verify that the randomization on the top page corresponds to that one indicated by the index i. In the voting phase, helper organizations assist the voter to audit ballots in the same way.

Voting

The voting authorities hand a blank ballot to the voter in a sealed envelope after verifying her eligibility. The voter can either use the blank ballot to vote or ask the authorities to audit it. In the latter case, the authorities publicly detach the scratch surfaces on the ballot and check the commitment (as before) through a computer. This procedure can be performed again by helper organizations that would employ their own computers. Assuming that the ballot is verified as well-formed, it is discarded and the authorities hand a new blank ballot to the voter. In principle, we could allow the voter to opt to audit a number of ballots before accepting one to use to cast her vote. If any ballot fails the audit checks, then recovery mechanisms need to be invoked. Discussion of this is beyond the scope of this paper.

To cast her vote, the voter performs the following steps (see also Figure 3):

1. (Selecting the option) In the voting booth, the voter chooses her option and marks the corresponding bubble on the ballot (a).

2. (Verifying the ballot) She separates the two pages of her ballot (b) and adds the bottom page into an envelope to make visible only the scratch surfaces. After this, she destroys in public the top page by means of a paper shredder (c) and hands the envelope containing the bottom page to the officials. They verify that the surfaces are whole.

3. (Casting the vote) The voter removes the bottom page from the envelope and casts it publicly into the Farnel box (d).

4. (Obtaining the receipt) After receiving the bottom page, the Farnel box removes the scratch surface that covers only the commitment value on the left side, shuffles its set of bottom pages (e), and copies one of them. The copies are held by the voter as her receipt (f).

Note that the scheme may employ a mechanism to prevent voters from destroying top pages other than their own. For example, the ballots could be numbered in a similar way as in the case of preventing chain voting attacks (see Jones [Jon05] for details).

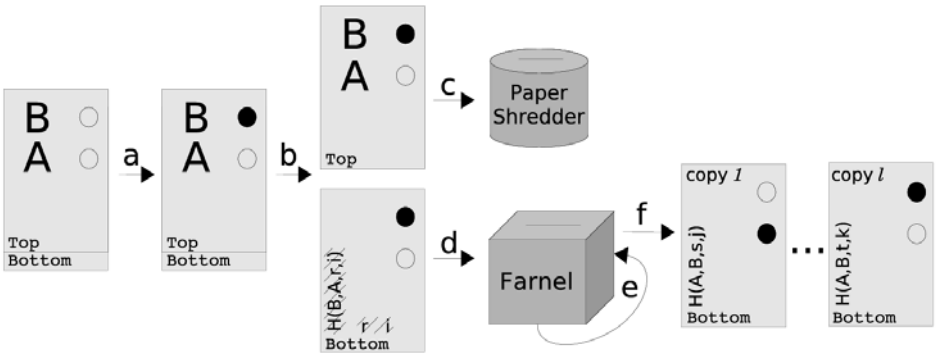


Figure 3: The main voting steps of the single box Farnel scheme.

Recovering and Tallying the Votes

In order to tally the votes, the talliers open the Farnel box, detach the scratch surfaces on all votes, and publish the votes on the bulletin board. Then, the talliers start the process to recover the votes. In this process, they compare the index on the vote with the index on the bulletin board to identify the permutation of the options; remember that the permutations as well as their indexes were previously published. From the permutation identified and the mark on the ballot, the talliers determine the option chosen by the voter. After recovering the votes, the authorities open all commitments using the random numbers and the indexes. In this step, they hash the random number and the index along with the permutation identified before, and compare the resulting hash with the hash on the vote. Now, the talliers count the votes in the same way as Farnel, that is, all votes are counted and the votes cast during the initialization phase are subtracted from this sum.

Verifying the Votes

Voters can, as usual, visit the bulletin board and confirm that their receipts appear accurately, and complain if they are not. Particularly, they verify the commitments and the marks on their receipts correspond to those on the votes published on the board. Helper organizations and observers verify that the talliers performed their work correctly.

4.2.1 Human Readable Paper Audit Trail

In the manner of Ryan [Rya07], the scheme could be adapted to provide a HRPAT by employing a conventional ballot box as alternative to the paper shredder. This way, instead of destroying the top page in a paper shredder, this page may be cast into the conventional ballot box. The box would store the top pages as an audit trail so that the votes can be counted without depending on the votes from the Farnel box.

5 Conclusions

We have presented a new ballot design for the scheme of Araújo et al. and a new voter-verifiable scheme based on Farnel. The solutions rely on the Prêt-à-Voter style ballots and cryptography to achieve security. Despite employing cryptography, the proposals require only a hash function and the voters perform simple steps to verify the votes corresponding to their receipts. That is, they just match numbers (i.e. hashes) and the marks on their receipts with the votes on the board. Helper organizations perform a more thorough verification of the hashes.

Moreover, we have introduced a novel way to initialize the Farnel box that employs void ballots. This initialization, however, only works with the ballot forms that give rise to protected receipts with a void option, e.g., Prêt-à-Vote style ballots. The new process would be easier to monitor and verify than having to maintain and record the total of the various votes cast in the initialization phase. Even so, ensuring only void votes are cast during the initialization phase is still challenging and will require carefully designed monitoring procedures.

Implementing the concept of the Farnel box in a way that requires minimal trust in the mechanism or procedures remains challenging. Rivest employed the original Farnel idea to overcome the reconstruction attack in the version of the Threeballot proposed in [Riv06]. In his scheme, a copy of a vote is made in advance and then it is exchanged by means of Farnel. This may be proved easier to implement with less trust assumptions. However, to prevent any possibility of the voter wandering off with her original receipt, the two steps (i.e. copy and exchange) need to be performed in close proximity.

An interesting feature of the Farnel mechanism is that it may help counter certain psychological style attacks on voter-verifiable schemes in which voters are convinced that the secrecy of their vote is not guaranteed. Using Farnel, the voters do not retain their own receipts, so any fear that the vote can be extracted should be mitigated. The down-side is that voters may be less motivated to check receipts if the receipt they hold is not their own. This may be offset by ensuring that voter helper organizations are on hand to perform the checks on behalf of the voters. If voters are given more than one receipt each this should also help as long as a reasonable proportion of voters are diligent enough to check all or many of their receipts.

Besides helping counter psychological attacks, the Farnel idea also mitigates randomization style attacks. These attacks were introduced by Schoenmakers [Sch00]. To perform a randomization attack, the adversary instructs the voter to generate a receipt that has a certain property. The adversary will not know what vote will be encoded, this is effectively random. The effect then is to force voters to vote for a random candidate, so nullifying their right to vote freely. The attack can be applied to Prêt-à-Voter and to Punch Scan schemes as the voter receipt in these schemes contain the position chosen by the voter. This way, an adversary may ask the voter to place her X in a specific position and to show him afterwards the receipt marked in this position. By means of the Farnel idea, however, the voter exchanges her receipt before leaving the voting place. Thus, the adversary cannot verify that the voter followed his instructions.

References

[ACvdG07] Roberto Araújo, Ricardo Felipe Custódio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel. IAVoSS Workshop On Trustworthy Elections (WOTE'07), June 2007.

[AR06] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pages 29–40, New York, NY, USA, 2006. ACM.

[CRS05] David Chaum, Peter Y. A. Ryan, and Steve A. Schneider. A Practical Voter-Verifiable Election Scheme. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, ESORICS, volume 3679 of Lecture Notes in Computer Science, pages 118–139. Springer, 2005.

[Cus01] Ricardo Custódio. Farnel: um protocolo de votação papel com verificabilidade parcial. Invited Talk at Simpósio Segurança em Informática (SSI), November 2001.

[Jon05] Douglas W. Jones. Chain Voting, August 2005. http://vote.nist.gov/threats/papers/ChainVoting.pdf.

[PH06] Stefan Popoveniuc and Ben Hosp. An Introduction to Punchscan. IAVoSS Workshop On Trustworthy Elections (WOTE'06), June 2006.

[Riv06] Ronald L. Rivest. The ThreeBallot Voting System. http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pd%f, October 2006.

[RR06] Brian Randell and Peter Y.A. Ryan. Voting Technologies and Trust. IEEE Security and Privacy, 04(5):50–56, 2006.

[RS07] Ronald Rivest and Warren Smith. Three Voting Protocols: ThreeBallot, VAV, and Twin. Electronic Voting Technology Workshop (EVT'07), August 2007.

[Rya04] P.Y.A. Ryan. A Variant of the Chaum Voting Scheme. Technical Report CS-TR-864, University of Newcastle upon Tyne, 2004.
[Rya07] P.Y.A. Ryan. Pret a Voter with a Human-Readable, Paper Audit Trail. Technical Report CS-TR-1038, University of Newcastle upon Tyne, 2007.
[Sch00] Berry Schoenmakers. Personal communication, 2000.

Session 6: Certification of E-Voting

Development of a Formal IT Security Model for Remote Electronic Voting Systems

Rüdiger Grimm[1], Melanie Volkamer[2]

[1]Forschungsbereich IT-Risk-Management
Universität Koblenz-Landau
grimm@uni-koblenz.de

[2]Institut für IT-Sicherheit und Sicherheitsrecht
Universität Passau
volkamer@uni-passau.de

Abstract: Remote electronic voting systems are more and more used - not so much for parliamentary elections, but nevertheless for elections on lower levels as in associations and at universities. In order to have a basis for the evaluation and certification, in Germany a Common Criteria Protection Profile [PP08] is developed, which defines basic requirements for remote electronic voting systems. This Protection Profile requires a rather low evaluation depth (EAL2+). For elections on higher levels an appropriate adjustment of the evaluation depth is recommended. In its first part this paper points out that increasing the evaluation depth beyond EAL5 is not possible at present, since EAL6 requires formal methods and in particular a formal IT security model. Such a formal model does not exist yet. In the second part, this paper proposes a first step to an IT security model for remote electronic voting systems, which, however, considers only a subset of the security objectives defined in the Protection Profile [PP08].

1 Introduction

Over the last two years, the Gesellschaft für Informatik (GI – the German society of computer scientists) has developed a Protection Profile (PP) for a basic set of security requirements for remote electronic voting systems [PP08] in cooperation with the Bundesamt für Sicherheit in der Informationstechnik (BSI – German Federal Office for Information Security) and the German Research Center for Artificial Intelligence (DFKI). The Protection Profile is based on the Common Criteria [CC06]. It defines a minimum set of security objectives, which every remote electronic voting system has to ensure and a set of assumptions to the environment, in which the system is used. A remote electronic voting system certified against this Protection Profile [PP08] assures a secret, free, equal and universal election only under the condition that the system is used in an environment where the defined assumptions hold.

The Common Criteria (CC) together with the Common Evaluation Methodology [CEM06] define how the compliance of a particular system with the defined security objectives has to be evaluated. The CC differentiates between different evaluation depths. They distinguish between evaluation assurance level (EAL) 1 to 7+, whereby 7+ means the most intensive evaluation. Generally, the deeper this evaluation goes, the higher is the trustworthiness into the certified system. The scope of the system to be evaluated, the evaluation complexity, and the evaluation methods rise with rising EAL level. The Protection Profile, which defines a basic set of security requirements for remote electronic voting systems, requires the assurance level EAL2+ which is characterised by the following aspects:

- Execution of independent and structured tests by the evaluator
- Analysis of the documentation up to the high-level design and the interface specification
- Analysis of the strength of the functions
- Search for obvious vulnerabilities by the evaluator
- Presence of a configuration system
- Evidence of secure system delivery procedures

EAL2+ is certainly sufficient for elections in associations, schools and universities, but not for elections on higher levels and in particular not for parliamentary elections. Thus, for example, the persons in charge of the Protection Profile, which define requirements for the digital election pen[36] [PP06][37], require EAL3+[38]. Some critics demanded EAL4 and even higher.

[36] The digital election pen had been planned for the citizenry election in Hamburg in February 2008.
[37] The Protection Profile is based on the Common Criteria version 2.3.
[38] The Protection Profile required EAL 3 augmented with the following components: ADV_SPM.1 (Informal TOE security policy model) and AVA_MSU.3 (Analysis and testing for insecure states) - replacing AVA_MSU.1.

In the past, systems have been predominantly evaluated according to evaluation assurance levels equal or below EAL4+, since starting from the EAL5 semi-formal and/or formal methods are required. The application of such methods causes substantial additional effort for manufacturers and evaluators. The decision for such a high evaluation assurance level should be made before starting the development because (semi-)formal methods cannot be implemented in the follow-up (the effort to do so in the follow-up is as large as a complete new development). However, EAL5 provides a substantial increase in the trustworthiness of certified systems compared to EAL4, because a semi-formal description of the system design as well as a more modular and therefore better analysable architecture is demanded. A corresponding increase can be identified from EAL5 to EAL6 because the semi-formal specification languages are replaced by formal specification languages. ”Past experiences show that a formal modelling of the security policies given as a formal security model may lead to an increase of confidence in the security of the product that obeys these security policies.” [DFKI02]

Starting from EAL6, the Common Criteria component ADV_SPM.1 has to be ensured, which demands the use of a formal IT security model. Moreover, the component requires a consistency proof (in form of a mathematical proof) for the model itself and a compliance conformance between the system specification and the defined model. To do so, it is possible to use already published and established formal IT security models[39] as a whole or in parts. If no suitable formal IT security model exists, such a model must be developed.

The latter case holds for remote electronic voting systems. Therefore, such a formal IT security model has to be developed before an evaluation according to EAL6 and/or 7 can be aimed. In the context of this article we point out, by the example of some concrete security objectives defined in the Protection Profile, how such a formal IT security model can be designed.

In the further contribution, the definition of an IT security model is introduced (see chapter 2), then it is discussed whether existing IT security models can be applied (see chapter 3). Subsequently, security objectives from the Protection Profile are identified, which are considered for the definition of a formal IT security model (see chapter 4), and afterwards a formal IT security model is developed and proven to ensure all characteristics of an IT security model (see chapter 5). The paper closes with the proposal of future work activities and a short summery (see chapter 6).

[39] Examples for available and established IT security models are: Bell/LaPadula model, the Clark Wilson model, and the Biba model.

2 IT Security Model (General Introduction)

Model Definition. According to [Grimm08], IT security models define system states and state transitions, differentiate between secure and insecure states, and explain under which circumstances secure states are reached. An IT security model can be more or less formal. All IT security models contain the following *five description elements*:

1. The definition of a superior security objective
2. The specification of secure system states[40] which represent together the superior security objective
3. A trust model, describing a set of assumptions about the environment in which the system is used and under which the set of secure system states is equivalent to the superior security objective.
4. A set of permitted state transitions
5. A security theorem, claiming that applying any permitted state transitions to any secure state necessarily transfers to a secure state again.

Explaining the Coherences. An IT security model has to close the following two gaps:

- between the secure system states and the superior security objective (trust model in 3) and
- between the permitted state transitions and the secure system states (security theorem in 5).

For our purpose the first gap is already closed by the Protection Profile; in particular by

- the security problem definition, including a list of assumptions about the environment,
- the list of security objectives for the system, and
- the discussions in section „security objective rationale".

Therefore, this aspect is not further discussed in this paper. The second gap is closed by the security theorem with its corresponding proof in sections 4 and 5 of this paper.

[40] The specification of secure system states corresponds to the Common Criteria security objectives (in case of a non formal IT security model).

Definition of Secure System States and Permitted State Transitions. The secure states (description element 2) and the permitted state transitions (description element 4) have to be described as accurately and precisely as possible. One informal way to formulate secure states is the definition of security objectives according to the Common Criteria [CC07]. In this case, the security theorem (description element 5) is proven by a linguistically convincing and conclusive argumentation. For applications which require a high security assurance, the definitions of a secure state and of permitted state transitions must be consistent and the corresponding security theorem must hold without any doubt. In this case, it is necessary to specify the secure states and the permitted state transitions in a formal way, and the security theorem must be proven with mathematical means. The formal specification of both together (in description elements 2 and 4) together with the formal proof (in description element 5) represents a *formal IT security model*[41].

In the case of a formal IT security model, a third gap has to be closed - the gap between the linguistically formulated security objectives from the Protection Profile and the formal specification of the secure states. This cannot be formalised, but this is the subject of an argumentative discourse of security and application experts.

Advantages of the Application of Formal Methods. The application of formal IT security models has three main advantages:

- No natural language can guarantee an unambiguous interpretation and, therefore, it provides no feasibility to prove consistence in the formulation of secure states and permitted state transitions. Vulnerabilities in the implementation of these are a consequence. In contrast, the application of mathematical established technical equipment, which makes the application of computer-aided proofs possible, enables the definition of unambiguous and inter-subjective secure states and permitted state transitions.

- The development of a formal IT security model is used to identify and remove inconclusive, inconsistent, contradictory, or not enforceable secure states and/or permitted state transitions which cannot be detected with natural language.

- Using natural language for the specification of secure states and permitted state transitions causes similar problems for the evaluator - it is hard and in general not unambiguous to decide whether the implemented security functions are sufficient to ensure the specified secure states and permitted state transitions. Based on a formal specification of the system, it can be formally proven that the specification and later the implementation conform to the formal specification of the secure states and permitted state transitions.

[41] The Common Criteria defines formal security models in the following way: "A formal security model is a precise formal presentation of the important aspects of security and their relationship to the behaviour of the TOE; it identifies the set of rules and practises that regulate how the TSF manages, protects, and otherwise controls the system resources. […] the formal security policy model is merely a formal representation of the set of SFRs being claimed." [CC06]

3 Application of Available IT Security Models for elections

To our knowledge, no formal IT security model is available which completely covers the superior security objective of a secure remote electronic election. Caused by the numerous different tasks of a remote electronic voting system, the existence of such a model also seems to be unrealistic. However, the integrity model of Clark Wilson [CW87] and the confidentiality model of Bell-LaPadula [BLP73] can possibly describe partial security objectives.

The Clark Wilson model introduced the separation of duty principle to security modelling. For different partial security objectives in the context of a remote electronic voting system, it might be possible to use the separation of responsibilities in the sense of Clark Wilson. The Protection Profile defining basic security requirements for remote electronic voting systems [PP08] demands, for example:

> ***O.AuthPollworkers****: The TOE implements an authentication function which supports the separation of duty principle for at least two members […]. Thus, at least two poll workers control each other.*

This PP security objective corresponds to the certification rule C3 and the penetration rules E2 and E3, which describe the "internal consistency" of a system in the Clark Wilson model:

- E2: The system has a list mapping users to transaction procedures (user X, TPi, (CDIa, CDIb, CDIc, …)) and ensures that users can only execute transaction procedures according to this list.
- C3: The allocation list from rule E2 complies with the separation of duty principle.
- E3: The system authenticates the user's identity before executing any transaction procedure.

The Bell-LaPadula model prevents confidential information flow to public domains. This is achieved by mandatory access control. This approach could conceivably structure voters, poll workers, ballots and the ballot box in a hierarchical information flow model a là Bell-LaPadula and, thus, to model the secrecy of the vote. These approaches are still open research tasks.

The following chapters will discuss other security objectives defined in the Protection Profile, which cannot be modelled with Bell LaPadula, Clark Wilson or none of the other well-known formal IT security models. Therefore, a new formal IT security model is developed for these PP security objectives. The developed transaction procedures for the penetration of these security objectives could be embedded into a superior separation of duty model according to Clark Wilson. This integration needs to be further analysed in the context of future work.

4 Selection of PP Security Objectives

The development of a formal IT security model for remote electronic voting systems is a complex task and happens gradually by adding security objectives, defined in the Protection Profile, step by step. The security model, which will be presented in chapter 5, is a first step accomplished for two selected security objectives from the Protection Profile defining basic security requirements for remote electronic voting [PP08]. This first step illustrates how the further security objectives can be specified formally. The two selected security objectives are:

> **O.UnauthVoter**: *Only eligible voters who have been unambiguously identified and authenticated are allowed to cast a vote that is stored in the e-ballot box.*
>
> **O.OneVoterOneVote**: *It is ensured that (A) each voter can cast only one vote and that (B) no voter loses his voting right without having cast a vote. [….].*

5 Formal IT Security Model for Remote Electronic Voting

Different possibilities to model a particular system exist. According to [Grimm08] an IT security model for the above identified security objectives can be described in the following way:

Definition of the Superior Security Objective (1). Execution of a secure, equal, universal, direct, secret, and free remote electronic election.

Definition of a System State. A system state is represented by a triple of the following three entries:

1. W – Set of eligible voters (those who are listed in the electoral register and have not yet cast a vote).
2. S – Set of (encrypted) votes stored in the e-ballot box.
3. $voter: S \rightarrow M$ – Mapping (encrypted) votes on their electors.
   M is a superset of W_{total}, that is, $M \supseteq W_{total}$. M contains any user who tries to access the remote electronic voting system, whether or not this particular user has the right to cast a vote. The function *voter* assigns each (encrypted) vote to its producer (voter).

   Remark 1: in the case of postal voting, the function *voter* is realised by the outer envelope which is labelled with the sender's name and address. During the tallying phase, the sender information is checked and is verified whether $voter(s) \in W_{total}$ or $voter(s) \in M \backslash W_{total}$. In the first case, the outer envelope is removed and the inner one containing the vote is put into the ballot box, while in the second case the envelope is destroyed.

Remark 2: the values of *voter* are visible only for the last vote (or votes) cast into the e-ballot box, i.e., only for the $s \in S_{i+1} \setminus S_i$. After anonymising S, the values of *voter* cannot be reconstructed. Therefore, in praxis, the *voter* mapping should only be used during state transitions on the $s \in S_{i+1} \setminus S_i$. Secure state transitions are controllable on this "visible subset" $S_{i+1} \setminus S_i$ of S_{i+1} only (see rules for permitted state transitions (4) below). For the "invisible part" S_i of the *voter* mapping on S_{i+1} we define $voter_{i+1}|S_i := voter_i$.

Initial State. $< W_{total}, S_0 = \{\}, voter_0 = \{\} >$ is the initial state.

W_{total} stands for the set of all voters in the electoral register (those who have already cast a vote and those who still have the right to cast a vote). The two empty sets S_0 and $voter_0$ stand for the empty e-ballot-box in the beginning and the corresponding empty mapping of the empty box on the users of the voting system.

Specification of Secure States (2). It has to be defined which properties represent a secure state. According to chapter 4, the PP security objectives O.UnauthVoter and O.OneVoterOneVote are selected to be specified in terms of formal state properties denoting a secure state:

- **O.UnauthVoter:** $\forall s \in S: voter(s) \in W_{total}$**;** that is, the e-ballot box contains only those e-votes ($s \in S$) from which the corresponding elector ($voter(s) \in Wtotal$) is listed in the electoral register. In order to ensure this, the voter needs to be unambiguously identified and authenticated.
- **O.OneVoterOneVote: (A)** $\forall s, s' \in S: voter(s) = voter(s') \Rightarrow s = s'$**;** that is, whenever the set S of cast votes contains two votes from the same voter, then these two votes are identical. Thus, only one of the stored e-votes is tallied. This means that each voter can cast only one vote.

  (B) $\forall x \in W_{total} \setminus W: \exists s \in S: voter(s) = x$**;** that is, a voter can only become an elector if his e-vote is stored in the e-ballot box ($s \in S$). Thus, he cannot lose his right to vote without having cast a vote which has been successfully stored in the e-ballot box.

Remark It is easy to prove that these three conditions for a secure state are equivalent to the following two conditions: "$W_{total} = W + voter(S)$" (where "+" denotes the disjoint union of sets) *and* "The *voter* mapping is injective." An alternative way to prove the security theorem (5) would be to prove that these two conditions are implied by the permitted state transitions (4). However, we prefer to derive our three conditions of a secure state (2) directly from the following permitted state transitions.

Trust model (3). The set of assumptions about the environment and the corresponding reasoning are part of [PP08].

Permitted State Transitions (4). A state transition from state $Z_i=<W_i, S_i, voter_i>$ to $Z_{i+1}=<W_{i+1}, S_{i+1}, voter_{i+1}>$ is permitted if one of the following rules holds:

- State transitions in which no vote is cast:
  [rule 1] $W_i = W_{i+1} \wedge S_i = S_{i+1} \wedge voter_i = voter_{i+1}$

- State transitions in which a vote is cast and successfully stored in the e-ballot box, that is, the sets S and W are modified:
  [rule 2] $\exists s \in S_{i+1} : (voter_{i+1}(s) \in W_i \wedge W_{i+1} = W_i \setminus \{voter_{i+1}(s)\} \wedge S_i = S_{i+1} \setminus \{s\})$

Remark 1: All $m \in M$ can initiate a state transition by casting a vote. However, for not permitted state transitions holds: $m \in M \setminus W_{total}. \Rightarrow W_{i+1} = W_i$ and $S_{i+1}=S_i$.

Remark 2: The state transition rules use the *voter* mapping only on its visible part, that is, on $S_{i+1} \setminus S_i$. This makes the transition rules usable in praxis.

Theorem (5). For all permitted state transitions starting with the initial state, $Z_0=<W_{total}, \{\}, \{\}>$ holds that any reachable state is a secure state.

Proof. The theorem can be proven by mathematical induction. To simplify our notation, we write *voter* instead of $voter_{i+1}$ or $voter_i$, we understand that $voter_{i+1}|S_i:=voter_i$. To simplify the main proof, it is helpful to first prove that for all permitted state transitions Z_0 to Z_i the following three lemmas L1, L2 and L3 hold. These are now named and proven:

L1: $S_i \neq S_{i+1} \vee W_i \neq W_{i+1} \Rightarrow \exists s \in S_{i+1}: (S_{i+1} \setminus S_i = \{s\} \wedge W_i \setminus W_{i+1} = \{voter(s)\})$

Interpretation: *During each permitted state transition according to [rule 2] exactly one new vote is generated and exactly the one associated voter loses his right to vote.*

Proof for L1: In the case $S_i \neq S_{i+1} \vee W_i \neq W_{i+1,}$ [rule 2] had to be applied. Therefore, there exists an $s \in S_{i+1}$ for which holds: $S_i=S_{i+1} \setminus \{s\}$: Thus s is the only element in $S_{i+1} \setminus S_i$. Therefore, the first part of the lemma is proven. Moreover, according to [rule 2] the following statement holds for this s: $voter(s) \in W_i$ with $W_{i+1}=W_i \setminus \{voter(s)\}$. Thus, *voter(s)* is the only element in $W_i \setminus W_{i+1}$. Therefore, the second part of the lemma is proven.

q.e.d. (L1)

L2: $W_{total} = W_0 \supseteq W_1 \supseteq W_2 \supseteq \ldots \supseteq W_i$

Interpretation: *The set of eligible voters can only decrease.*

Proof for L2: This lemma is a trivial consequence of [rule 2].

q.e.d. (L2)

L3: $\forall s \in S_i : \exists j < i : voter(s) \in W_j \backslash W_i$

Interpretation: *For each vote stored in the e-ballot box, there exists a voting right discarded earlier.*

Proof of L3: Application of proof by induction over *i*, starting with *i=1:*

Induction Base: For *i=1*: Choose *j=0*, then this case is equal to the special case of L1 with S_1 and S_0.

Induction Hypothesis: L3 holds for some $i \geq 0$

Induction Step: For *i+1* holds:

$\forall s \in S_{i+1}$ does either hold $s \in S_{i+1} \cap S_i$ or $s \in S_{i+1} \backslash S_i$. In the first case the statement is true according to the induction hypothesis. In the second case, L1 proves the statement.

q.e.d. (L3)

Back to the main Proof:

- *Induction Base:* All three secure state properties do hold for the initial state Z_0 because S_0 and $W_{total} \backslash W_0$ are equal to the empty set.
- *Induction Hypothesis*: The secure state property holds for some state Z_i, $i \geq 0$.
- *Induction Step*: It needs to be shown that for all possible states Z_{i+1} reachable by permitted state transitions from Z_i holds that a secure state is reached:
  - [rule 1] $W_i = W_{i+1} \wedge S_i = S_{i+1}$; thus $Z_i = Z_{i+1}$. Therefore, applying the induction hypothesis it holds that also Z_{i+1} is a secure state.
  - [rule 2] $\exists s \in S_{i+1}: (voter(s) \in W_i \wedge W_{i+1} = W_i \backslash \{voter(s)\} \wedge S_i = S_{i+1} \backslash \{s\})$

We prove each of the three properties of a secure state separately:

O.UnauthVoter:

Induction Hypothesis: For some $i \geq 0$ holds: $\forall s \in S_i$: $voter(s) \in W_{total}$

Induction Step: Then for *i+1* holds:

$\forall s \in S_{i+1} : s \in S_{i+1} \cap S_i \wedge s \in S_{i+1} \backslash S_i$.

- Case $[s \in S_{i+1} \cap S_i]$: this holds because of the induction hypothesis.
- Case $[s \in S_{i+1} \backslash S_i]$: according to L1 holds: $W_i \backslash W_{i+1} = \{voter(s)\} \Rightarrow voter(s) \in W_i$ and according to L2 holds: $W_i \subseteq W_{total}$, hence $voter(s) \in W_{total}$.

q.e.d. (O.UnauthVoter)

O.OneVoterOneVote(A):

Induction Hypothesis: For some $i \geq 0$ holds: $\forall s,s' \in S_i$: $voter(s)=voter(s') \Rightarrow s=s'$

Induction Step: Then for $i+1$ holds:

For all s and s' only the following three possibilities exist:

- Case [$s, s' \in S_{i+1} \cap S_i$]: this holds because of the induction hypothesis.
- Case [$s, s' \in S_{i+1} \setminus S_i$]: according to L1 holds: $S_{i+1} \setminus S_i = \{s\} \Rightarrow s=s'$
- Case [$s \in S_{i+1} \setminus S_i, \wedge \; s' \in S_i$]: according to L1 holds: $W_i \setminus W_{i+1} = \{voter(s)\} \Rightarrow voter(s) \in W_i \setminus W_{i+1}$ and according to L3 holds $\exists j < i : voter(s') \in W_j \setminus W_i$
  Thus, $voter(s) \in W_i$ and $voter(s') \notin W_i$. Thus, both values can never be equal. Thus, the statement holds also in this third case.

q.e.d. (OneVoterOneVote(A))

O.OneVoterOneVote(B):

Induction Hypothesis: For some $i \geq 0$ holds: $\forall x \in W_{total} \setminus W_i$: $\exists s \in S_i$: $voter(s) = x$

Induction Step: Then for $i+1$ holds: For $x \in W_{total} \setminus W_{i+1}$, x must be in one of the following sets:

- Case [$x \in (W_{total} \setminus W_{i+1}) \cap (W_{total} \setminus W_i)$]: this holds because of the induction hypothesis.
- Case [$x \in (W_{total} \setminus W_{i+1}) \setminus (W_{total} \setminus W_i)$]: according to L2 holds: $W_{total} \supseteq W_i \supseteq W_{i+1}$. Thus, $(W_{total} \setminus W_{i+1}) \setminus (W_{total} \setminus W_i) = W_i \setminus W_{i+1}$; thus, $x \in W_i \setminus W_{i+1}$; in addition, it holds: $W_i \neq W_{i+1}$. According to L1 holds $W_i \setminus W_{i+1} = \{voter(s)\}$ for $s \in S_{i+1} \setminus S_i$. Then, deduced from $x \in W_i \setminus W_{i+1}$ it holds: $voter(s)=x$; this completes the proof for $i+1$.

q.e.d. (OneVoterOneVote(B))

All together: q.e.d. (Theorem)

6 Future Work and Summary

Currently, a Protection Profile (PP) defining basic security requirements for remote electronic voting [PP08] is accomplished in Germany. This PP demands the evaluation assurance level EAL2+. The current discussions about the evaluation of electronic voting systems in general illustrate that the critics demand a high EAL level. We agree because political elections are the highest property of a democracy. Therefore, we believe that formal methods are well motivated for voting applications. However, concerning an evaluation according to EAL6 or EAL7 there are still a couple of open questions and research tasks to solve (not only concerning remote electronic voting). It is necessary to further discuss the specification of IT security models for remote electronic voting systems.

This contribution demonstrates with two examples how security objectives, defined by the basic profile PP can be integrated into a formal IT security model. Up to a complete formalisation of all security objectives and their integration in a closed IT security model for remote electronic voting systems, substantial research has to be carried out.

Acknowledgements

We thank Dieter Hutter for his helpful comments on our formalisation method.

References

[CC06] Common Criteria for Information Technology Security Evaluation, Version 3.1, 2006.

[CEM06] Common Methodology for Information Technology Security Evaluation, Version 3.1, 2006.

[DFKI02] H. Mantel, W. Stephan, M. Ullmann, and R. Vogt. Leitfaden für die Erstellung und Prüfung formaler Sicherhetismodell im Rahmen von ITSEC und Common Criteria. Version 1.0c http://david.von-oheimb.de/cs/teach/BSI-Leitfaden_1.0c.pdf, 2002

[Grimm08] R. Grimm, IT-Sicherheitsmodelle. Arbeitsberichte aus dem FB Informatik der Universität Koblenz-Landau, Feb 2008, erscheint in WISU

[PP06] M. Volkamer and R. Vogt. Digitales Wahlstift-System. Common Criteria Protection Profile BSI-PP-0031, http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf, 2006.

[PP08] M. Volkamer and R. Vogt. Core Requirements for Online Voting Systems. Protection profile, German Research Center for Artificial Intelligence, 2008.

[CW87] D. Clark and D. Wilson. A Comparison of Commercial and Military Security Policies. Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, CA. Computer Society Press of the IEEE, Washington DC, 184-194, 1987.

[BLP73] D. E. Bell and L. J. LaPadula. Secure Computer Systems: Mathematical Foundations, and A mathematical model. ESD-TR-73-278, MTR-2547, Vols 1&2. The MITRE Corporation, Bedford, MA, Nov 1973.

The Certification of E-Voting Mechanisms. Fighting against Opacity

Jordi Barrat i Esteve

Dpt. Estudis Jurídics de l'Estat / R+D (SEJ2007-64886)
University of Alacant
Cta. Sant Vicent del Raspeig s/n
E-03690 Sant Vicent del Raspeig
jordi.barrat@ua.es

Abstract: Many countries are using certification procedures to guarantee the full compliance of e-voting mechanisms with democratic standards, but the data generated by these analysis is normally handled almost secretly. Given that transparency is a key principle to guarantee citizen's confidence in the electoral process, this opacity would only be acceptable after a correct balance of the concurrent interests. The paper provides specific data on the certification mechanisms of some countries and assesses the feasibility of a disclosure of the certification reports.

1 Introduction

Electronic voting raises several concerns, like, for instance, whether it can provide the same degree of electoral transparency and citizen control that already exists in our current elections. It is not clear how it can guarantee a meaningful recount similar to the traditional one based on paper ballots given that one of the main problems of any electronic voting solution is that an average citizen cannot easily understand how it is working. The current electoral structure allows everybody, even a person without specific skills, to check the accuracy of the process, but unfortunately the electronic voting platforms, at least if they have no paper trail, will never achieve the same degree of external supervision. Its implementation, therefore, should be to strengthen by supplementary control measures, so that, although different from the traditional ones, it would emulate the current framework so that the citizenry could have enough confidence in these new electoral devices.

Although there are different solutions to this problem (e.g. open source e-voting platforms), one of these new mechanisms could be a certification process. They already exists with the traditional paper voting systems, but they become much more important if applied to electronic voting platforms. The electoral authorities would only agree to voting machines that, according to several technical analyses, comply with detailed conditions previously set up. This process would be quite similar to the certification of industrial products, but here there are some specific features because we are not trying to check only whether a device is technically correct. We are also trying to compensate for the lack of citizen control that exists where voting procedures accept computer components. Moreover, ordinary industrial products generate external evidences of their performance, but electronic voting solutions cannot provide these external data because they must also guarantee the secrecy of the vote.

There are several items to be analysed in a certification procedure. The first one could be to decide who will actually carry out the technical analysis that any certification process entails (i). We should opt between public or private bodies and we could also analyse which criteria have been used for each appointment and the detailed conditions and terms to conduct this task. We could also wonder which components of the voting machines will be checked (ii). Once again, the landscape is very different depending on the country. We could find very detailed lists of requirements to be checked by the certification institutions, but also very ambiguous and generic documents. A third focus point could be the legal rules about the disclosure of the reports issued by the certification bodies and the availability of the overall file, that is, the technical documentation of the voting machine (e.g. source code) (iii). Following the patterns of the ordinary industrial certification processes, these policies use to be very opaque.

Due to length restrictions, this paper will only provide an overview of the third point. The analysis includes a preliminary theoretical approach in conjunction with detailed references of some real cases of binding electronic voting systems, namely in Belgium, Estonia, Netherlands (Internet voting not included) and France (Internet voting not included). However, a full understanding of the problem would also require taking into account the approaches developed in other countries like, for instance, the United States, Venezuela or Brazil.

2 The Certification Reports: How to Handle Sensitive Data

The credibility of a system such as electronic voting is supported by a combination of measures designed to increase its openness. The certification is one of these measures, but its actual effects will largely depend on the disclosure of its final findings and it is worth noting that, except for some slight nuances, in all the cases which have been observed, the decision taken was to restrict to the maximum the access to the documentation produced by the technical analysis.

Thus, we should not place too many expectations on the efficacy of the certification measures, at least strictly from the citizen's point of view. There is no doubt that such measures are thought to carry out a correct supervision, but, if such an obscurity is kept, they will by no means be able to emulate the openness and popular control guaranteed by the traditional voting systems. We shall analyse below the situation observed in several countries, paying special attention to the arguments put forward in order to deny access to the aforementioned documentation and also to certain situations where the possibility to achieve a wider spread seems to be making its way.

The French case is particularly interesting, since the public authorities had to take a position regarding a request by which a citizen expressly demanded the disclosure of the certification reports related to the three authorized voting companies. On February, 3rd 2006 the French Ministry of the Interior refused to grant such a claim following the criteria provided by the CADA –*Commission d'Accès aux Documents Administratifs*—. The CADA is an advisory body whose mission consists precisely on deciding, in the light of the regulations on the access to public information, which documents can be actually disclosed and, on the basis of different criteria, which must be handled in a different way. This Commission recommended not to disclose the requested documentation, arguing that it could be detrimental to "le secret industriel et commercial ... [et] compromettre le bon déroulement des élections" (the commercial and industrial secrecy ... [and] endanger the correct electoral management).[42]

Two reasons are given. The first one (i) emphasizes the rights of the private companies which take part in the process, pointing out that the disclosure of the documentation could be detrimental to their interests, specifically to their commercial and industrial secret. Please note that we are referring to the two companies involved and not only to the one that undertakes the development of the computer applications. This fact implies that both would be at risk, on the one hand, the control over the voting technological solution, and, on the other hand, the internal certification methodology used by the company responsible for drafting the report.

From my point of view, an ideal solution must take into account these legitimate interests, but it must also avoid considering them to be the only important interests in this field. As it has been pointed out before, electronic voting does not have the same features as other areas where the certification reports are normally secret. The reports related to many industrial products are subject to these opaque rules, but the electronic voting has a peculiarity that consists in the fact that it is impossible to verify whether the system really works properly. For instance, it will be relatively easy to prove that an authorized train does not meet the analysed parameters, since external evidences will appear. If an authorized train fails to reach the speed that it should theoretically achieve according to a previous technical document, it is obvious that someone has failed—either the railway company or the certification authorities.

[42] Document available at: www.ordinateurs-de-vote.org/IMG/jpg/cada.jpg [September 7th 2007].

Unfortunately, this method cannot be used in the electronic voting field. In view of the fact that the vote is secret, and unless we decide to implement a paper receipt, there is no external evidence beyond the computer audit that allows us to assert that the results obtained by means of the electronic system faithfully reflect the voter's will. As a matter of fact, the scandals arising from some electronic voting applications, such as the those caused in Sarasota (Florida) or in Schaerbeek (Belgium), are based on absolutely illogical results, as, for instance, the recording of an unusually high rate of abstentionism in a given election[43] or a vote distribution that is incompatible with the electoral formula.[44] These extreme cases may in fact be inspected, and such has been the case, but nothing can be done in other less dramatic cases that would happen, for instance, if the electoral fraud consisted only in shifting the direction of a vote in each constituency.

Thus, the legal framework, which supports the certification of the electronic voting, must rest on this basis and not, as usually happens, on the false premise that the general guidelines for the certification of other products are also applicable in this field.

The ideal solution would obviously consist in enforcing the public and general disclosure of these reports, but before reaching such a stage, it is advisable to examine the possibility of finding an intermediate solution which may not only satisfy the companies involved, but which could also be especially beneficial for the openness required by any electoral system.

[43] In 2006, Christine Jennings lost her seat as a representative by a very few votes, but in Sarasota County something strange happened and more than 10% of the voters, even though they had attended the polling station and had voted in many of the simultaneous calls for elections that usually take place in the United States, surprisingly decided to abstain from the election for the House of Representatives, which is one of the most important calls. Moreover, if we compare this percentage with that obtained in the neighbouring region, we will easily prove that the citizens who behaved in a similar way in such a region were many fewer on a relative footing. Further information at: Division of Elections / Florida Department of State - http://election.dos.state.fl.us/CongressDistrict13.shtml [September 15th 2007].

[44] To be specific, a candidate obtained a number of preferential votes that exceeded the votes received by the list of candidates in which he was included. There was a difference of 4096 votes. The Collège des Experts, together with the company involved and the Ministry of the Interior itself, pointed out that the most probable reason "pouvait être attribuée à une inversion spontanée d'une position binaire dans la memoire vive du PC ... Un écart de 4096 peut être occasioné par une inversion de la 13ème position binaire du compteur" (could have been a spontaneous inversion of a binary poristion within the live PC memory ... A difference of 4096 [votes] could be generated by an inversion of the 13rd binary position of a counting device) [Co03, p.19]. The existence of a physical endorsement for each vote in the form of magnetic cards made it possible to repeat the counting and, in view of the fact that this technical incident did not happen again, they opted to accept the second results as valid. However, this does not make what happened less serious and it raises the question of what the solution would have been in the event that there had been no magnetic cards.

We may consider first whether the very premise on which we rely is certain, that is, whether the belief that disclosing these reports will unavoidably entail an irreparable harm for the industrial and commercial property rights of the companies involved. As a matter of fact, stating that this belief is certain, at least in such a convincing and general way, is far from reflecting the reality. There are several factors that must be taken into account and that may make this statement more flexible in certain respects. One of these factors consists in requiring certain previous certification parameters, which must be detailed and comprehensive and must even include the method to be used for the verification. This is what happens in France, where the electronic voting systems must accredit that a total of 114 conditions of different kinds are met. One of the sections included in the certification reports will obviously consist in a detailed review of these requirements and the integration of the corresponding comments regarding the fact of whether or not the voting prototype has passed the tests.

If the circumstances are as described, the risk of revealing important trade and business secrets seems to be quite remote, and thus, allowing at least a partial disclosure of the certification reports would be reasonable. We should bear in mind that sometimes the comments will not just consist in an affirmative or a negative remark, but they will provide some additional information and these are the details which will precisely help strengthen the electoral openness and the trust of the citizens. The incident that occurred in France regarding the internal clock of NEPAD's machines is a perfect example of what has been stated.[45]

[45] As a result of a lawsuit brought in Vaucresson, the Ministry of the Interior disclosed part of the report that Bureau Veritas had drafted for NEDAP [available at: www.ordinateurs-de-vote.org/IMG/pdf/nedap_20070412_veritas.pdf (September 7th 2007)]. The issues at stake were, on the one hand, the hypothetical contradictions between the devices manufactured by NEDAP, which had been purchased at that time in Vaucresson, and on the other hand, some of the conditions which were required by the technical regulations on which a report had to be delivered by the certification authorities, to be specific by Bureau Veritas.

Thus, for instance, the 6th requirement establishes that the members of the polling station must be able to "régler l'horloge interne de la machine à voter" (adjust the internal clock of the e-voting machine) and to the same effect the 46th requirement states that such adjustment must rely on "les données heure-minute-seconde" (the data hour-minute-second). The aim of both conditions is to get devices able to "dater les divers évenements et comptes-rendus mémorisés au cours d'un scrutin" (fix the temporal data of the different actions and memos saved during the election) (46th requirement) and, subsequently, the final printings produced by the voting machine must include "les heures d'ouverture et de clôture du scrutin" (opening and closing hours of the election) (19th requirement). Another important issue was the locking mechanism of the voting system, since the 7th requirement envisages "un double dispositif d'authentification électronique" (a double electronic authentication device).

To begin with, from my point of view, it is difficult to assert that the pages that were sent to court compromise the trade secrets of NEPAD or *Bureau Veritas*. In both cases the pages only contained some three-column tables where, together with a tag regarding each requirement demanded by the legal regulations, *Bureau Veritas* had included a comment to the effect of whether or not the prototype complied with each legal condition. Should there be any doubt about the interpretation of the legal regulations or about the total or partial compliance with them, as in the clock's case, the certification authority shall reflect the results obtained and describe as minor or major discrepancies the differences that have been found. All-in-all, we are dealing with documents which neither uncover a computer's architecture nor explain in detail the internal methodology of *Bureau Veritas*, but still they can be extremely helpful for the citizens to get an exact idea of how an electronic voting system works.

For instance, in the internal clock's case, the most important fact is not so much whether or not the machine has an absolute or a relative timer, an argument which was, by the way, rejected by the *Conseil d'État*[46] as well as by the *Conseil Constitutionnel*.[47] The important fact is that now reading the report lets us know that the machine did not really comply with all the legal requirements and that the certification company as well as the Ministry itself had to resort to the cunning argument that the discrepancies were minor in order to be able to validate them.[48]

[46] As a result of an appeal lodged in Versailles, the Conseil d'Etat solved this question as follows: "Considérant ... que le règlement technique fixant les conditions d'agrément des machines à voter impose seulement que les machines soit dotées d'une horloge interne que le bureau de vote puisse régler lors de son initialisation et qui permette le chronométrage des évènements du scrutin, mais n'exige pas que ce réglage et ce chronométrage soient opérés directement en fonction de l'heure légale; que par suite il est manifeste que le système d'horodatage 'relatif' retenu par les concepteurs de ces machines ne méconnaît pas les conditions d'agrément des machines à voter" (Taking into account ... that the technical document is only requiring an internal clock for each voting machine that could be adjusted by the polling staff during the opening and that allows the chronological counting of the actions generated during the election, but it does not require a counting linked to the official hour; it is thus obvious that the relative counting foreseen by the computer scientists fully complies with the conditions for the acceptance of the voting machines) (Ordonnance no. 305184 from May 2nd 2007).

[47] The Conseil Constitutionnel literally accepted the judgement given by the Conseil d'Etat and, on the basis of the same objection, dismissed an appeal lodged in Aulnay-sous-Bois as a result of the parliamentary elections held in June [Decision 2007-3449 from July 26th 2007]. May I draw your attention to the fact that the argument related to the existence of a mechanical key does not seem to have been used either in the litigation before the Conseil d'Etat or in the one before the Conseil Constitutionnel.

[48] Diverse mechanisms are used in order to deal with the literal sense of the technical requirements, although they all have a common origin, which is some discrepancy between the voting system subject to analysis and the legal requirements. Sometimes the strategy consists in acknowledging some minor discrepancies which, therefore, would not compromise a general positive assessment. This is what happens with the mechanical key problem (7th requirement) and, setting aside the classification of the incident as serious or slight, with the implementation of a relative clock (6th requirement).

However, sometimes the certification authority agrees that the corresponding requirement has been met, even though the previous comments logically lead to a different conclusion. Such is the case, for instance, of the 19th requirement which states that the documents generated by the computer contain all the data "exceptées les heures d'ouverture et fermeture, qu'il convient d'ajouter à la main" (unless the opening and closing hours, that should be manually added) (the italics are mine). The surprising fact is that, as it was pointed out before, according to the technical document, these data related to time are precisely the data which must be printed.

This detail could only become known as a result of the publication of the extract sent to court, since it was not included in any of the previous public statements. In this sense, a wider spread of these tables which, as has been said before, do not compromise the commercial interests of the companies, could provide the citizens with a more complete and detailed sight of the certification process, of the possible implications of the discrepancies, and of the criterion used by the certification authorities in order to classify them as minor or major discrepancies. Although most of the citizens actually lack technical knowledge, such data would allow them to have a better-grounded opinion on whether or not the certification process has been properly designed to perform its purpose, that is to say, to verify whether or not the electronic voting system observes the basic principles of any democratic election.

Other parameters to be taken into account consist in identifying which players will actually receive the sensitive data of the e-voting company and under which conditions. If we implement a certification process, the vendor is accepting to provide sensitive data to a third party, that is, the certifying body, and it seems therefore feasible that other stakeholders might have access to the same information or, at least, to the final report generated by these certification activities. Obviously the vendor could require some conditions, like a confidentiality agreement similar to the one already accepted by the certification body, but there should be no obstacle to broaden the recipients of this information to research groups, to professional corporations or to given civil society organizations closely related to these topics. It would not be a full openness, that could barely guarantee a minimum of confidentiality, but we are managing to involve some supplementary stakeholders. We maintain the same confidentiality conditions already implemented, but we enhance the principle of transparency.

If we analyse the praxis in some countries, we will easily discover that the apparently strict confidentiality requirement is actually breached in some cases. *ES&S*, for instance, accepted during the last French presidential elections, a partial disclosure of its *Bureau Veritas* certification report to some customers belonging to local administrations because, in France, these bodies are actually deciding which e-voting supplier, among the three previously authorized, is the best one. These representatives were invited to *ES&S* headquarters where they could read –not copy— the report. If the vendor itself is implementing such protocols, it would hardly be acceptable not to provide the same information with the same conditions to other stakeholders that seem to be at least as important as local authorities. I am referring, for instance, to political parties.

Belgium is an interesting example, although we will also find some paradoxes. While the source code is largely spread, the certification reports, apparently less dangerous information, are handled with great opacity. The source code is delivered to the political parties even before the elections, although they have to respect a confidentiality agreement. Their IT experts could therefore analyse the system and communicate to the Ministry of Interior whatever mistakes they have found. Second, the electoral authorities upload the full source code to the website immediately after the elections.[49]

[49] See a technical analysis carried out by aFRONT based on the source code used in 2003 and 2004: www.afront.be/lib/vote.html (September 15th 2007).

This transparent behaviour hardly matches with the treatment provided to the results of the certification activities. It would be difficult to reject the publication of the certification report on the grounds of risks for the industrial property, because the source code will already be known by the citizenry. Following the aforementioned Fresh arguments, we could also argue that what is actually in danger is the methodology of the certifying institution, but we already know that this parameter could have minor relevance if the criteria are previously set up in a very detailed way. Unfortunately, Belgium does not meet this condition because the criteria are not detailed and therefore the certifying bodies have large powers to assess whether the software complies with them.

This opaque approach may have unwanted consequences since the citizenry could become more and more reluctant to easily accept the fair behaviour of the electoral authorities. It is worth recalling, for instance, the following statement of the *Collège des Experts*: "Il est à noter que l'attitude du SPF Interieur vis à vis les rapports des organismes d'avis est fort peu critique. En effet, peu importe la qualité des tests, un rapport positif est visiblement accueilli avec un gran soulagement" (It is worth noting that the Ministry of Inteior's behaviour is not very rigorous regarding the reports issued by the certifying companies. Despite the actual quality of the checks, a positive report is publicly received with a great relief) [Co07, p. 16]. The only way to avoid this perception is to accept a full disclosure of the certification report and the *Collège* actually makes this recommendation later [Co07, p. 28].

The Netherlands also has a nuanced framework that does not match with the simple and quick French solution. The *Brightsight's* report was kept secret during the 2006 elections, but the implementation of the Act regarding a free access to the public information allows the disclosure of significant data about the relationships between the electoral authorities and their computer supplier *Groenendaal* [Wv07]. The certification report is not publicly available yet, however.

Finally, assuming that Estonia does not have a formal certification procedure [DM02, p. 238], its electoral authorities accepted in 2007 several verifications carried out by specialists, but unfortunately "the results of these reviews were not made public" [Os07, p 15]. The private audit, carried out during the electoral period aiming to check whether the operational protocols were correctly followed, is not publicly available either [Os07.p. 15].

There are therefore some interesting paradoxes. While the system seems to be very open, accepting reviews carried out by any interested group, the subsequent decisions are very opaque because the findings of these procedures remain secret. Is it actually useful, from a democratic point of view, to foster such confidentiality agreements? Obviously these reviews are important achievements, mainly if we take into account what is happening in other countries, but their usefulness is not clear since we will not be able to alert the society to the vulnerabilities that we could have found.

It is difficult to find balanced solutions in these cases, but we could try to soften confidentiality agreements so that any person could at least publicly provide a general overview of his/her analysis confirming the system's reliability or pointing out some weaknesses. The first statement will definitively strengthen the citizen's confidence and the second one, even in these generic terms, will likely rouse citizen's concerns and will foster further check ups by the electoral authorities themselves.

Finally, there was a second argument (ii) within the CADA's recommendation. A full disclosure of the certification reports "pourrait compromettre le bon déroulement des elections." Certainly, one common argument against open source is the risk to provide sensitive information to external hackers. Although this is a technical debate and this paper only has a legal approach, it is worth underlining that many computer scientists, even perhaps a large majority, are actually supporting open source solutions as the best ones. Jason Kitkat, for instance, thinks that a disclosure is not neutral and actually increases the system's security: "Cryptographers and security professionals use peer review to provide assurance for the quality of their systems. A security scheme whose source code and design is known yet continues to offer a useful level of protection is a good one" [Ki04, p. 65; same opinion Ru06, p. 125]. There will be other challenges, like the verification that all the devices are actually containing the correct code, but the security and robustness of the product would be enhanced with an open strategy.

3 Concluding Remarks

The certification of industrial components used to be an ordinary procedure thought to guarantee their quality and security within a standardized protocol of supervision mechanisms. However, electronic voting platforms have some specific features, like the need to maintain the transparency of any electoral step and the lack of a paper trail that, if required, could allow us to perform a second tally. Since the certification process should take into account these specific needs, we should profile a special protocol for this single product. Although there are several items to analyse: who is doing the technical analysis (i), which criteria should be used (ii) and who should receive the final reports (iii), this paper is only focused on the third one.

The protection of the industrial property has been so far a common argument to reject a full disclosure of the certification reports. It is a legitimate position, but it should be balanced with other approaches given that we are talking about electoral processes and therefore the citizens' confidence in the system should be a major outcome. A fair business concurrence might also be a sound argument against opacity. Should e-voting systems increase their implementation worldwide? Should new or more balance between transparency and property be sought? Despite the current framework, the paper shows how some minor data coming from given countries actually suggests that the opacity is not well grounded and that it would be easily feasible to include a certain degree of transparency without breaching the industrial property.

These humble measures could be a good beginning in order to achieve afterwards a new balance between electoral transparency and other opposite interests. Moreover, the Belgian experience should be seriously taken into account, because its structural weakness, the Collège des Experts, provides external control over the e-voting process.

References

[AH04] Álvarez, M.; Hall, T.: Point, Click and Vote: The Future of Internet Voting. The Brookings Institution, Washington, 2004.

[Co03] Collèges des Experts: Rapport concernant les élections du 18 mai 2003. Collège des Experts chargés du contrôle des systèmes de vote automatisés, [Brussels], 2003. www.poureva.be/IMG/pdf/RapportExperts2003.pdf [September 15th 2007]

[Co07] Collèges des Experts: Rapport concernant les élections du 10 juin 2007. Collège des Experts chargés du contrôle des systèmes de vote automatisés, [Brussels], 2007. www.poureva.be/IMG/pdf/RAPPORT_CONCERNANT_LES_ELECTIONS_DU_10_JUIN_2007.ocr.pdf [September 8th 2007]

[DM02] Drechsler, W.; Madisse, Ü.: E-Voting in Estonia. In: Trames. Journal of the Humanities and Social Sciences. n. 3, 2002; P. 234-244.

[Fe07] Fernández Rodríguez, J. J.: Voto electrónico. Estudio comparado en una aproximación jurídico-política (Desafíos y posibilidades). Fundap, Querétaro, 2007.

[Gr03] Gritzalis, D. A. (ed.): Secure Electronic Voting. Advances in Information Security. Kluwer, Boston, 2003.

[KB04] Kersting, N.; Balderstein, H. (eds.): Electronic Voting and Democracy: a Comparative Analysis. Palgrave Macmillan, Basingtoke, 2004.

[Ki04] Kitcat, J.: Source Availability and E-Voting: An Advocate Recants. In: Communications of the ACM. n. 47(10), 2004; P. 65-67. http://doi.acm.org/10.1145/1022594.1022625 [September 4th 2007]

[Kr06] Krimmer, R. (ed.): Electronic Voting 2006. (Col. "Lecture Notes in Informatics – LNI" / P-86), Gesellschaft für Informatik, Bonn, 2006..

[OS07] Osce: Republic of Estonia. Parliamentary Elections 4 March 2007. OSCE/ODIHR Election Assessment Mission Report. OSCE (The Organization for Security and Co-operation in Europe), Warsaw, 2007. www.osce.org/item/25385.html [September 15th 2007]

[PK04] Proser, A.; Krimmer, R.: Electronic Voting in Europe. Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, 2004.

[Ru06] Rubin, A. D.: Brave New Ballot. The Battle to Safeguard Democracy in the Age of Electronic Voting. Morgan Road Books, New York, 2006.

[TM05] Trechsel, A. H.; Méndez, F. (eds.): The European Union and E-Voting. Addresing the European Parliament's Internet Voting Challenge. Routledge, London, 2005.

[Tu05] Tula, M. I. (coord.): Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales. Ariel, Buenos Aires, 2005.

[Wv07] Wvsn: Voting systems company threatens Dutch state. Ed. Wij vertrouwen stemcomputers niet — WVSN, Amsterdam, 2007. www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal [September 2nd 2007]

Session 7: Technological Issues of E-Voting

Code Voting With Linkable Group Signatures

Jörg Helbach[1], Jörg Schwenk[2], Sven Schäge[3]

Chair for Network and Data Security
Ruhr-University Bochum
Universitätsstr. 150
D-44780 Bochum
[1]joerg@helbach.info
[23]{joerg.schwenk | sven.schäge}@rub.de

Abstract: Code Voting is an appropriate technology to deal with the "Secure Platform Problem" [Riv02]. However, code voting as proposed by Chaum [Cha01] is vulnerable to vote selling and other flaccidities. In this paper we describe the vulnerabilities of code voting and propose to extend code voting to prevent vote selling. For this purpose we combine code voting with linkable group signatures and vote updating. We analyze the security properties of this new approach.

1 Introduction

Regarding remote online voting systems one of the major issues is the security of the voting client, i.e. the personal computer of the voter, as it cannot considered to be trustworthy. Due to this fact in 2002 Ronald Rivest coined the term "Secure Platform Problem" [Riv02]. Even though different cryptographic voting protocols exist, the problem is that the voting client could be infected with malicious software, which is nowadays a widespread problem. Some estimates say that between 15% and 25% of all computers on the Internet are infected with malware bots [Web07], i.e. they have been under the complete control of an adversary. Hence, the voter cannot be sure that his electronic ballot is submitted faultless and unmodified to the voting server. Some methods for resolving this problem have been analyzed in [Opp02]. A good approach to overcome this problem is to use code voting as introduced by David Chaum in 2001 [Cha01]. Instead of a candidate's name, the voter only submits a voting transaction number (voting TAN) to the voting server. There is no correlation between the chosen candidate and the voting TAN on the voting client. So even if malware is installed on the client, it cannot identify the decision of the voter.

In this paper we will describe the code voting approach in detail and show that it is vulnerable against vote selling and denial of service attacks regarding the voting client. We then propose to improve code voting to deal with those vulnerabilities. Furthermore we combine code voting with vote updating and linkable group signatures. At last we describe the security properties of the new introduced approach.

2 Election Requirements

2.1 Security Requirements

In general voting systems used for (political) elections have to be free, universal, secret and equal. Much research has been done to adopt those requirements to remote online voting systems. Regarding Germany respectively Europe two important studies are the catalogue of requirements of the Physikalisch-Technische Bundesanstalt (PTB) [PTB04] and the recommendation of the Committee of Ministers of the Council of Europe [CoE04]. In 2006 Grimm et.al. analyzed those requirements and developed a protection profile for non-political elections according to the Common Criteria [GKM+06].

Summarized one can specify the following list of security requirements, which is not intended to be complete or comprehensive:

- Completeness and soundness of the Internet voting protocol(s),
- Correctness of the results
- Authenticity of both the voter (or the voting client acting on behalf of the voter, respectively) and the voting server,
- Secrecy of the ballots (including, for example, anonymity of the voter),
- Integrity of the ballots (including, for example, protection against malicious software)
- Non-duplication of the ballots,
- Availability and reliability of the voting process (including, for example, protection against denial of service attacks)

Even though single of those requirements are easy to fulfil, it is quite difficult to achieve all requirements concurrently, for some of them are contradictory. Furthermore appropriate cryptographic methods exist to deal with single requirements. E.g. to guarantee the secrecy of the ballot, one can use asymmetric encryption technologies. But as the encryption has to be computed on the voter's local client computer (in case of a remote online voting system), it is possible that malicious software forges the encryption process. As the local voting client is an important part of a remote online voting system and malware is an increasing problem on personal computers, it is difficult to ensure the client's security and integrity. As mentioned, therefore, in 2002 Ronald Rivest introduced the term “Secure Platform Problem” [Riv02]. We think that code voting, which we will describe in the next section is one (if not the only one) approach that works on a large scale.

2.2 Other requirements

Additionally to the security requirements there are further requirements, which a (electronic) voting system has to or should fulfil.

As mentioned above a political election has to be free, i.e. the voter must be able to vote for his favoured candidate without the fear of oppression or other disadvantages. The secrecy of the voter's ballot protects the freeness of his or her vote. Due to these facts a vote has to be anonymous, i.e. an attacker must not be able to correlate a (intercepted) ballot to a voter. Furthermore the voter must not be able, voluntary or nonvoluntary, to prove his vote to a third person to prevent vote selling or coercion of the voter. In the literature this property is named receipt-freeness.

Another relevant property of voting systems is the verifiability of the election process. In our democracy it is very important that the voter trusts this process and its result. This trust is often addicted to the possibility to check the election process in general and the calculation of the tally in particular. We distinguish between two kinds of verifiability, individual and universal verifiability. A voting system is individual verifiable, if the voter can check that his or her ballot has been computed in the tally correctly. Certainly the voter must be the only one, who can check his own vote. A voting system is universal verifiable, if it is individual verifiable and additionally all voters can check that the tally was calculated correctly. The particular challenge regarding individual and universal verifiability is not to compromise the receipt-freeness of the voting system.

3 The Secure Platform Problem

There is a simple attack against most of the remote voting systems proposed in the literature: If the attacker is able to control the communication channel between PC and voter, he can present the voting options in a different order, intercept the choice of the voter and redirect it to a voting option of his choice. This approach is similar to recent attacks on online banking systems [Gri03] [SW07] [LS07]. All cryptographic primitives employed can protect the voter’s choice only from the point where it has been entered into the PC. There are two major options to solve this problem:

- Securing the PC against malware, e.g. by using Trusted Computing techniques.
- Using a separate channel from the voting authority to the voter, e.g. by snail mail, or by using a stand-alone security token.

We propose to use code voting [Cha01], where the separate channel is instantiated by snail mail. However, this scheme is vulnerable to vote selling attacks, so to be able to use this scheme in political elections, we have to add additional functionality. This additional functionality will be a linkable group signature scheme that is executed inside the untrusted PC. This may at first seem contradictory, but the adversary does not gain an advantage by manipulating the GS scheme, as long as the private key of the group member remains secret.

4 Code Voting

The term code voting was introduced in 2001 by David Chaum [Cha01]. Each eligible voter is issued a code sheet as shown in table1.

Candidate	Voting TAN
Alice	738747987
Bob	983293774
Clark	192851911
…	…

Table 1: Printed Code Sheet.

As with many remote online voting systems, the voter connects to the remote voting server, but instead of submitting the name of his or her favoured candidate the voter only enters the appropriate voting TAN, i.e. if a voter wants to vote for Bob he just enters 983293774 into the voting application. Using code voting we assume

- a trustworthy voting authority, which issues a valid code sheet to every eligible voter, and
- the according voting servers and databases to be reliable and secure.

With the two additional requirements

- all voting codes are random and unique for every code sheet and every candidate, and
- the code sheets must not be distributed by electronically means

we can consider code voting secure against active and passive attacks [HS07]. In a passive attack the adversary can read the submitted voting TAN. As this voting TAN is random and there is no correlation between the voting TAN and the chosen candidate, the best the attacker can do is guessing the vote. In an active attack the adversary not only can read, but also could modify or discard the submitted voting TAN. For the attacker neither knows the corresponding candidate nor can calculate a new voting TAN, the best he can do is guessing again. However, code voting is vulnerable to unnoticeable denial of service attacks, as the attacker could prevent the voting client from submitting the chosen voting TAN to the server either by simply discard the voting TAN or modifying the voting TAN, so that it is invalid. The voter has no possibility to discover that his vote wasn't delivered to the voting server. For this purpose a possible extension of the basic code sheet is to introduce a confirmation TAN, which is displayed after the voting TAN was delivered correctly to the voting server as shown in table 2.

Voting TAN	Candidate	Confirmation TAN
738747987	Alice	332676873
983293774	Bob	676476488
192851911	Clark	301287123
…	…	…

Table 2: Printed code sheet with confirmation TAN.

After the voter entered the voting TAN and it was successfully delivered to the voting server, the server responds with the confirmation TAN. This confirmation TAN is also random and unique for every code sheet and every candidate, so the voter has evidence, that his chosen voting TAN was delivered correctly to the voting server. However, one has to think about the voter's claiming possibilities in case of a faulty or missing confirmation TAN. With this solution one possible (averaging) attack is to prevent the voter from voting by means of a denial of service attack, i.e. the voter enters the chosen voting TAN, but malware on the client computer prevents from submitting the voting TAN to the voting server. Then the malware either answers with a random, faulty confirmation TAN or doesn't answer at all. We then can assume, that the voter would enter another voting TAN (in particular when vote updating is allowed) to check, if his code sheet is correct. Presumably, the voter would then enter a voting TAN corresponding to an outsider candidate, which the malware allows to pass. However, this problem that neither the sender nor the receiver of a TAN could know, if his message was delivered successfully, is comparable to the two army problem [AEH75][Gra78], which illustrates the problems and challenges of attempting to coordinate an action of two parties over an unreliable communication channel. However, though one can show that the two army problem has no solution, often as a solution approach a three-way handshake is used, as e.g. used in TCP. According to this approach we propose a 3-step scheme by adding a third TAN, the finalization TAN (see table 3). The voting server only counts the vote, if the finalization TAN has been entered by the voter. With the attack described above, one can assume that the voter wouldn't enter the finalization TAN, if he or she doesn't receive the correct confirmation TAN.

Voting TAN	Candidate	Confirmation TAN	Finalization TAN
738747987	Alice	332676873	442367810
983293774	Bob	676476488	123456789
192851911	Clark	301287123	520172861
…	…	…	…

Table 3: Printed code sheet with confirmation and finalization TAN.

5 Vote Selling

However, even with a finalization TAN, code voting is vulnerable to vote selling, as the voter could simply sell the code sheet or a scanned copy thereof to an attacker. Even if vote updating is allowed and the vote seller tries to update his or her vote, he or she is racing with the vote buyer, and the vote buyer can arrange to be almost certain to win the race, since the vote buyer can re-perform the update as many times as needed. We have to assume that the vote buyer probably has more resources and patience than the vote seller, and, for instance, can automate the process of repeatedly sending updates.

In the following sections we will improve code voting with group signatures and vote updating to deal with vote selling.

6 Code Voting With Linkable Group Signatures

6.1 Group Signatures

In 1991 Chaum and van Heyst presented the concept of a group signature scheme [CH91]. A group signature is used to allow every member of a group sign messages on the group's behalf. In most cases those signatures are anonymous, i.e. it is not possible to identify which member of the group has signed a particular message. In addition, one cannot check if two signed messages were signed by the same group member. However, only a designated group manager exists who manages the membership list of the group and who can reveal the identity of the signer of a message.

6.2 Procedures in Group Signature Schemes

The group signature setting comprises three parties, namely the group manager M, the group members u_i and one or more verifiers w_j. In a group signature scheme, these parties participate in several polynomial-time algorithms (Fig. 1)[50]:

- GMKEY: a probabilistic algorithm that generates the private keys *isk* (issuing key) and *opk* (opening key) for M together with a group public key *gpk*.
- GUKEY: a probabilistic key generation algorithm that provides each user u_i with a public key pair (upk_i, usk_i). The key upk_i is also referred to as membership key or pseudonym and should only be known to u_i and M.
- JOIN: an interactive algorithm in which M computes a membership certificate v_i on *upk* for user u_i using *isk*. Using v_i, u_i can prove to any verifier w_j that he is a member of the group administered by M.

[50] We here omit the JUDGE procedure, assuming that each identity determined by the OPEN algorithm is accompanied with a proof of that fact.

- SIGN: a probabilistic algorithm in which u_i generates a signature s on an arbitrary message m using a membership certificate v_i and a secret key usk_i. Essentially, for a group signature scheme, no party can learn from s which v_i was used to generate it nor determine if any two signatures s and s' have been generated by the same group user.

- VERIFY: given gpk, m, and s a verifier w_j can use this deterministic algorithm to determine if a received signature s has actually been signed by a group member.

- OPEN: given opk and a message m with a corresponding group signature s, this deterministic algorithm can identify the originator of s.

A secure group signature scheme must guarantee the following (informal) security properties[51] [ACJT00]:

- Correctness: A group signature s, which has been correctly generated by a group user, is always accepted by a verifier.

- Unforgeability: only group users can generate valid group signatures.

- Anonymity: no one (except M) can learn the identity of the originator of a valid group signature.

- Unlinkability: no one (except M) can decide whether two signatures have been issued by the same user.

- Traceability: the group manager M can associate all valid group signatures with their originator.

- Coalition-resistance: a set C of malicious group users cannot work together to successfully create valid group signatures, which are associated to a user u_i who is not a member of C.

In [BSZ05] the security requirements of group signature schemes are reduced to just four basic properties (including correctness). Each property is then formalized in an attack experiment. Accordingly, a group signature scheme is called secure with respect to a certain security property if no polynomial-time attacker can win the corresponding experiment with a non-negligible probability.

[51] We remark that some authors even consider further security properties.

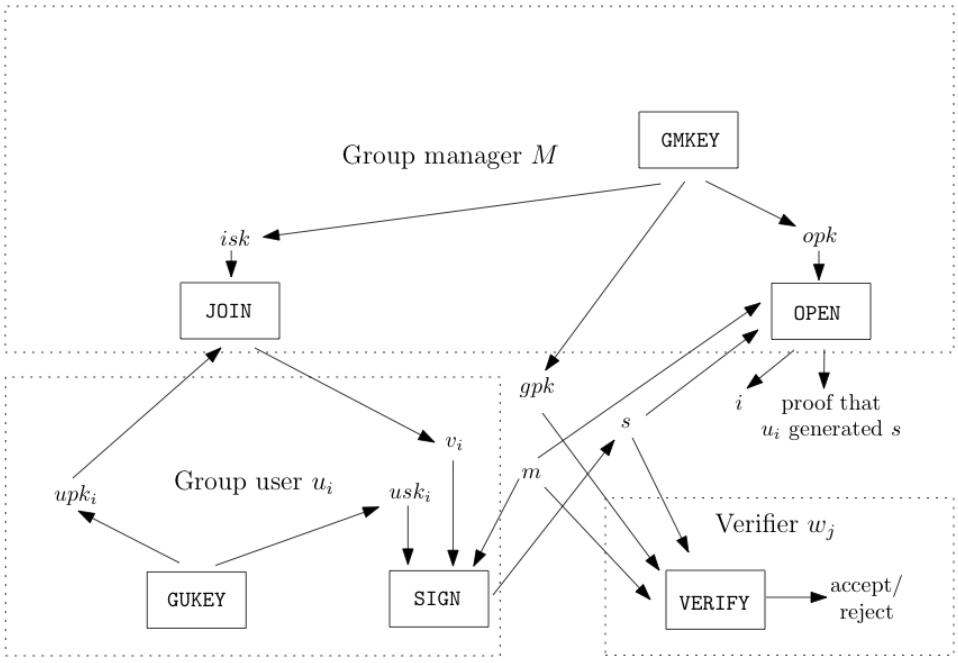


Figure 1: Group signature scheme. *gpk*: group public key; *isk*: (private) issuing key; *opk*: (private) opening key; usk_i: (private) user key; upk_i: membership key; *m*: message to be signed; v_i membership certificate; *s*: group signature on *m*; *i* user identity

6.3 Signatures of Knowledge

Signatures of knowledge are among the most important building blocks for group signature schemes. They are based on zero-knowledge protocols in which a prover can convince a verifier that he possesses a certain secret without revealing any information on that secret. Basically, usual 3-move zero-knowledge proofs of knowledge are made non-interactive using the Fiat-Shamir heuristic by replacing the verifier in the first two protocol steps with a hash function. Accordingly, the output of the hash function is interpreted as one or more challenges for the prover. The input to the hash function consists of the random commitments of the prover along with additional public information. In a signature of knowledge, these values are concatenated with the message to be signed. Signatures of knowledge can be proven secure in the random-oracle model. As a result, a signature of knowledge convinces a verifier that its issuer knows a certain secret while at the same time not revealing any information on that secret. Similar to [CS97] we denote signatures of knowledge rather descriptive than technical. According to this, a signature of knowledge of the fact that the issuer knows, for example, the discrete logarithms of y to the base g is denoted as:

$$SK\{(\alpha) : y = g^{\alpha}\}(m).$$

Such signatures of knowledge can easily be constructed using Schnorr signatures [Sch91]:

Let H: $\{0,1\}^* \rightarrow \{0,1\}^k$ be a collision-resistant hash function with a k-bit output and $G=\langle g\rangle=\langle h\rangle$ be a cyclic group of prime order p. Then, a signature of knowledge of the above fact is a pair

$$(c,d) \text{ in } \{0,1\}^k \times Zp^*$$

satisfying

$$c=H(m||y||g||g^d y^c).$$

Signatures of knowledge can also be used to prove more complex statements about secrets, like

$$SK\{(\alpha,\beta): y=g^\alpha \text{ and } z=h^\beta\}(m)$$

$$SK\{(\alpha,\beta): y=g^\alpha \text{ or } z=h^\beta\}(m)$$

$$SK\{(\alpha): y=g^\alpha \text{ and } \alpha \text{ is in } [A,B]\}(m).$$

The security properties of signatures of knowledge make them suitable for the design of SIGN algorithms. To show that he is a group user of *M*'s group, u_i has to prove that he (*i*) possesses a group membership certificate y_i issued by *M* and (*ii*) that he knows the private key usk_i corresponding to the public key upk_i certified in v_i. By showing his membership certificate or his membership key directly to a verifier, the user would make his signatures linkable. Using signatures of knowledge u_i can show possession of both values without actually revealing them. Essentially, u_i exploits that signatures of knowledge can be randomized (just like interactive zero-knowledge proofs of knowledge) by the prover. The group user only has to choose a new random commitment (corresponding to the first protocol move in an interactive zero-knowledge proof) every time he issues a group signature. In this way u_i can guarantee that no two signatures are equal, thus making the group signature scheme unlinkable.

6.4 Linkable Group Signatures

In 1997 Camenish and Stadler introduced the first efficient group signature scheme. Using this group signature scheme the length of the public key is independent from the size of the group. Even if a new member joins the group it is not necessary to calculate a new public key. Furthermore, in this scheme it is possible to assign the two different roles of the group manager (issuer of membership certificates and opener of group signatures) to different parties, which is a very desirable property regarding electronic voting systems. Since then, a large number of group signature schemes have been proposed [GW07]. We will show how to change such schemes to linkable GS schemes using the high-level description from [CS97]. Our starting point is to force each group user not to randomize his signatures of knowledge:

• The group manager M computes a key pair (sig_M, ver_M) of a digital signature scheme, and a public key encryption key pair (enc_M, dec_M), and publishes the two public keys.

• Alice joins the group by choosing a random value x, sending her membership key z=f(x) (f a one-way function) in an authenticated way to M, and receiving in return her membership certificate $v=sig_M(z)$.

• Alice signs a message m by encrypting (m,z) using the group managers encryption key, i.e. $d=enc_M(m,z)$. (Note: We omit the random number here to make the GS linkable.) She computes a signature of knowledge that she knows the values x' and v' satisfying the following equations: $d=enc_M(m,f(x'))$ and $ver_M(v',f(x'))=true$.

To protect the private key (x,z,v) against the attacker controlling the PC, this key can e.g. be bound to a TPM chip (which is much easier than to secure the whole platform using TPM technology), or it can be stored on a smart card (e.g. an electronic passport).

6.5 Vote Updating

To prevent vote selling in some voting systems, vote updating is used. That is, the voter could cast his or her ballot as often as he or she wants to, but only the last cast ballot is computed in the tally. The basic idea is that even if a voter sells his ballot to an attacker, he could easily update his or her vote. Hence the vote buyer never can be sure that the vote seller will not update his vote, after he has proven his choice to the vote buyer. E.g. the Estonian voting system, which was employed for the first political election over the Internet, uses vote updating [Est05]. Besides the advantages some disadvantages also exist. These advantages and disadvantages that are also different types of vote updating, are not further addressed in this paper, but are analyzed and discussed in [VG06]. However, we think that vote updating is a good method to prevent vote selling, but cannot be the only measure and therefore has to be facilitated by other measures [OSH08]. In this paper we will use vote updating as a part of a measure against vote selling, independent from the type of implementation of vote updating.

6.6 Improved Voting Scheme

To deal with vote selling and the secure platform problem, we propose to improve code voting. We assume a trustworthy voting authority, which consists of representatives of all parties that are supervising each other[52]. We further assume a group signature scheme as described in section 6.4. The voting authority is divided into different groups, which are responsible for the following tasks:

• Printing and issuing the code sheets to the eligible voters.

[52] In the literature, this property is called Separation of Duties.

- Operating the voting servers and the according databases, which we assume to be reliable and secure.
- Managing the group signature scheme by issuing the private keys to the eligible voters.
- Managing the group signature scheme by opening the signed voting TANs, i.e. verifying that every eligible voter only casts one ballot.

Each member of the voting authority should only belong to one of those groups.

The improved voting scheme works as follows: Prior to the election, each eligible voter is issued a private key according to the group signature scheme. Additionally, in a second step, the voting authority prints code sheets as seen in table 3. We assume that for every voter and every candidate the voting TANs, the confirmation TANs and the finalization TANs are randomly chosen using a good PRNG algorithm. Since the printing procedure links the voting TANs to the candidates, this process has to be monitored not only by the members of the code sheet issuing group, but by all voting authority members. For that purpose the different parties and their representatives in the voting authority then can check a control sample if the correlation between voting TAN and candidate is correct for the valid code sheets.

In a third step the valid code sheets are shuffled, put into anonymous envelopes and then they are distributed to the eligible voters. After the election has been started the voter connects to the voting server and enters the voting TAN for the desired candidate into the voting software and signs it with his private key according to the linkable group signature scheme. This signature could include information about e.g. the electoral district. The signed voting TAN is sent to the voting server over a MIX net. After the voting server has answered with the correct confirmation TAN, the voter approves his vote with the (signed) finalization TAN. In the improved code voting scheme we allow vote updating, i.e. every voter could submit several valid voting TANs to the voting server, but only the last submitted voting TAN approved with the corresponding finalization TAN counts in the tally. With the aid of the group signature, the responsible group of the voting authority ensures that a single voter can cast only one valid voting TAN regardless of how many code sheets he may have bought.

Therefore, this voting authority group opens the group signature to check if the voter already cast a ballot[53]. The finalized voting TAN is stored in the database, where older required voting TANs will be removed. If the voter gets either no or a faulty confirmation TAN, the client may be infected with malicious software, and he may vote again using another voting client, if the group signature scheme is transferable[54].

[53] For further research it would be interesting to analyze if threshold schemes could be applied in conjunction with the linkable group signature scheme, so that m out of n group managers are needed to open a signature.
[54] This is e.g. the case if the private key is stored on a smart card.

It is an open question whether at the end of the election the voting authority should publish the submitted voting TANs: since they are checkable also by a coercer, even if vote selling is impossible, the adversary may control the voting decision of certain voters.

7 Security Properties

A passive adversary is only able to attack the secrecy of an election. He can observe the TANs entered into the web browser. Since those TANs were chosen at random, the best an attacker can do is guess the vote. Additionally, in our voting scheme the voter sends his signed voting TAN to the server. As his or her vote is sent over a MIX net, an allocation between IP address and the submitted voting TAN is not possible. Even though malware on the voting client could just read the voting TAN, it cannot identify the chosen candidate. So our voting scheme is secret.

Further, our voting scheme is equal because the group signature is linkable by the group managers, i.e. for every eligible voter only one signed voting TAN is counted in the tally. If the voting scheme doesn't publish the submitted voting TANs, the proposed voting scheme is receipt free, but it is not verifiable. Because our voting scheme uses linkable group signatures, a vote buyer can only cast as many ballots as he has different group signature keys. For that purpose, the group managers have to issue a private key, which a voter presumably would not give to an attacker, e.g. a private key according to an ePass.

8 Summary

In this paper we proposed to use code voting as a reasonable measure against the "Secure Platform Problem" that is a major threat to most of the proposed electronic voting schemes. As the code voting model is vulnerable against vote selling, we extended code voting using vote updating and linkable group signatures to prevent vote selling attacks regarding the voting client and described some security properties of the new approach.

References

[ACJT00] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In Advances in Cryptology – CRYPTO 2000, vol. 1880 of Lecture Notes in Computer Science, pages 255–270. Springer 2000.

[AEH75] E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber. Some Constraints and Tradeoffs in the Design of Network Communications. In ACM SIGOPS Operating Systems Review, volume 9, pages 67–74, 1975.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In Topics in Cryptology - CT-RSA 2005, volume 3376 of Lecture Notes in Computer Science, pages 136–153. Springer-Verlag, 2005.

[Cha01] D. Chaum. Sure Vote: Technical Overview. In Proceedings of the workshop on trustworthy elections (WOTE '01), http://www.vote.caltech.edu/wote01/pdfs/surevote.pdf, 2001.

[CS97] J. Camenisch and M. Stadler. Efficient Group Signature Schemes for Large Groups. In Advances in Cryptology - CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 410–424. Springer-Verlag, 1997.

[CvH91] D. Chaum and E. van Heyst. Group signatures. In Advances in Cryptology – EUROCRYPT'91, volume 547 of Lecture Notes in Computer Science, pages 257–265. Springer-Verlag, 1991.

[Cyb05] Cybernetica. General description of the estonian e-voting system, online available under http://www.cyber.ee/english/services/eGovernment/evoting.html, 2005.

[GKM+06] R. Grimm, R. Krimmer, N. Meißner, K. Reinhard, M. Volkamer, M. Weinand, and J. Helbach. Security Requirements for Non-political Internet Voting. In Proceedings of the 2nd International Workshop on Electronic Voting 2006, volume 86 of Lecture Notes in Informatics, pages 203–212, 2006.

[Gra78] Jim Gray. Notes on Data Base Operating Systems. In Lecture Notes in Computer Science, volume 60, pages 393–418, 1978.

[Gri03] Roger A. Grimes. An SSL trojan unmasked. http://www.infoworld.com/article/06/03/03/75970_10OPsecadvise_1.html, 2003.

[HMR04] Volker Hartmann, Nils Meißner, and Dieter Richter. Online Voting Systems for Nonparliamentary Elections – Catalogue of Requirements. Technical Report PTB-8.5-2004-1, online available under http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf, Physikalisch-Technische Bundesanstalt, April 2004.

[HS07] Jörg Helbach and Jörg Schwenk. Secure Internet Voting with Code Sheets. In EVoting and Identity, First International Conference, VOTE-ID E-Voting and Identity, First International Conference, VOTE-ID, pages 166–177, 2007.

[LS07] H. Langweg and J. Schwenk. Schutz von FinTS/HBCI-Clients gegen¨uber Malware. In Proceedings of D-A-CH Security, pages 227–238, 2007.

[oE04] Council of Europe. Legal, operational and technical standards for e-voting. http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf, 2004.

[Opp02] R. Oppliger. How to Address the Secure Platform Problem for Remote Internet Voting. In Proceedings of the 5th Conference Security in Information Systems (SIS 2002), pages 153–173, http://www.ifi.unizh.ch/˜oppliger/Docs/sis_2002.pdf, 2002. vdf Hochschulverlag.

[OSH08] R. Oppliger, J. Schwenk, and J. Helbach. Protecting Code Voting Against Vote Selling. In SICHERHEIT 2008 - Sicherheit, Schutz und Zuverl¨assigkeit, volume 128 of Lecture Notes in Informatics, pages 193–204, 2008.

[Riv02] R. Rivest. Electronic voting. In Financial Cryptography '02, volume 2339 of Lecture Notes in Computer Science, pages 243–268. Springer-Verlag, 2002.

[Sch91] C. P. Schnorr. Efficient Signature Generation by Smart Cards. In Journal of Cryptology, volume 4, pages 161–174. Springer-Verlag, 1991.

[SW007] Secure Works: Win32.Grams E-Gold Account Siphoner Analysis. http://www.secureworks.com/research/threats/grams/, 2007.

[VG06] M. Volkamer and R. Grimm. Multiple Casts in Online Voting: Analyzing Chances. In Proceedings of the 2nd International Workshop on Electronic Voting 2006, volume 86 of Lecture Notes in Informatics, pages 97–106, 2006.

[Wan07] Guilin Wang. Bibliography on Group Signatures, http://icsd.i2r.a-star.edu.sg/staff/guilin/bible/group-sign.htm, 2007.

[Web07] T. Weber. Criminals 'may overwhelm the web, http://news.bbc.co.uk/1/hi/business/6298641.stm, 2007.

CAPTCHA-based Code Voting

Rolf Oppliger[1], Jörg Schwenk[2], Christoph Löhr[2]

[1]eSECURITY Technologies
CH-3073 Gümligen
rolf.oppliger@esecurity.ch

[2]Ruhr-University Bochum
D-44780 Bochum
{joerg.schwenk|christoph.loehr}@rub.de

Abstract: Code voting provides an appropriate technology to address the secure platform problem of remote Internet voting, but it is not particularly user-friendly. In this paper, we propose the use of CAPTCHA- an acronym standing for Completely Automated Public Turing tests to tell Computers and Humans Apart - to improve the user-friendliness of code voting, discuss the security of CAPTCHA-based code voting, and elaborate on a possible implementation.

1 Introduction

Elections and votes are fundamental processes for the proper operation of democratic states and their (democratically legitimated) governments. In the literature, the term *electronic voting* (or *e-voting* in short) is used to refer to elections and votes that are supported by electronic means. With the proliferation of the Internet, its use for e-voting has been proposed by many people (mainly politicians) as a way to make voting more convenient andas it is hopedto increase participation in elections and votes. The term *Internet voting* is therefore used to refer to election or voting processes that enable voters to cast their ballots over the Internet. This basically means that the ballots must be represented electronically, and that the electronic ballots must be transmitted to election officials using the Internet as a transport medium.

There are many possibilities to implement Internet voting, and poll-site Internet voting, Kiosk voting, and remote Internet voting are usually distinguished in the literature (e.g., [Cal00]). In this paper, we only focus on remote Internet voting, i.e., Internet voting where the voter (or a third party acting on behalf of the voter) uses his personal computer (PC) to cast a ballot over the Internet. From a security viewpoint, remote Internet voting is the most challenging possibility to implement Internet voting. In states that support absentee balloting, such as all-postal voting, any other form of Internet voting (i.e., poll-site Internet voting and Kiosk voting) is likely to fail. This is because the other possibilities require the voter to visit a voting place, and this is probably too inconvenient compared to the simplicity of casting ballots from home. In Europe, for example, a few states have started to employ remote Internet voting, be it in geographically restricted pilot projects, such as in three cantons of Switzerland [Ber08], or for official use, such as in Estland.

Against this background, it is possible and likely that the use of remote Internet voting tends upwards, and that the security of remote Internet voting will become a major issue. Security, in turn, has many aspects, and there are several partly complementary security technologies, mechanisms, and services that can be used to address them. As argued in [Opp02], code voting, i.e., voting by providing randomly-looking codes instead of YES or NO in the case of a vote and candidates' names in the case of an election, is an appropriate technology to address the secure platform problem of remote Internet voting. Unfortunately, code voting is not particularly user-friendly, and in this paper we exlore possibilities to use *Completely Automated Public Turing tests to tell Computers and Humans Apart* (CAPTCHAs) also known as *Reverse Turing Tests* (RTTs) or Human *Interactive Proofs* (HIPs) to improve the user-friendliness of code voting. We think that CAPTCHA-based code voting provides an interesting possibility to implement code voting in a real-world setting.

The rest of the paper is organized as follows: The security requirements of (remote) Internet voting are summarized in Section 2. Code voting and CAPTCHA-based code voting are introduced and discussed in Sections 3 and 4. A preliminary security analysis is given in Section 5. Finally, conclusions are drawn and an outlook is given in Section 6.

2 Security Requirements

There are many investigations and studies that elaborate on the security of Internet voting in general, and remote Internet voting in particular (e.g., [Cal00, Rub01]). The results all give evidence that security (including privacy and reliability) is among the most important preconditions for the successful deployment of Internet voting. The current paper ballot systems set a standard that is adopted as a security baseline for Internet voting. They represent certain tradeoffs between voter convenience and protection against fraud and abuse. It is generally required that elections and votes conducted over the Internet are at least as secure as the current paper ballot systems. In states that support absentee balloting in the form of all-postal voting, however, it is this voting technology that sets the security standard for Internet voting.

There are many lists of security requirements for (remote) Internet voting that can be found in the literature[55]. There is even an e-voting protection profile for the Common Criteria drafted in Germany[56]. The following list of security requirements is not intended to be complete or comprehensive:

- Completeness and soundness of the Internet voting protocol(s);
- Correctness of the results;
- Authenticity of both the voter (or the voting client acting on behalf of the voter, respectively) and the voting server;
- Secrecy of the ballots (including, for example, anonymity of the voter);
- Integrity of the ballots (including, for example, protection against malicious software);
- Non-duplication of the ballots;
- Availability and reliability of the voting process (including, for example, protection against denial-of-service attacks).

Some security requirements are complementary and don't interact with each other (e.g., integrity and non-duplication of the ballots). Other security requirements, however, are (or at least seem to be) contradictory in some sense. For example, one way to attest the correctness of a voting process is auditability, meaning that the entire voting process can be audited in some reasonable way. Auditability, however, sometimes contradicts to the secrecy of the ballots. In fact, there is a lot of research going on in the cryptographic community to address this apparent contradiction and to guarantee ballot secrecy and the correctness of the results simultaneously. Most of this research elaborates on schemes and protocols for verifiable secret sharing and secure multi-party computation as pioneered by Yao [Yao82].

[55] In 2004, for example, the Committee of Ministers of the Council of Europe adopted Recommendation Rec(2004)11 that specifies "legal, operational and technical standards for e-voting." These standards, among other things, also comprise security requirements.
[56] http://www2.dfki.de/fuse

Many security requirements of (remote) Internet voting can be addressed with existing technologies, mechanisms, and services. For example, there are many technologies that can be used to secure the server side. Examples include firewall technologies and intrusion detection systems (IDS) or intrusion prevention systems (IPS). The authenticity of the voter and the voting server can be addressed with public key certificates. Similarly, the secrecy and integrity of the ballots can be guaranteed with a cryptographic protocol, such as the Secure Sockets Layer (SSL) [FKK96] or Transport Layer Security (TLS) [DR06] protocol. It is, however, important to note that the use of the SSL/TLS protocol protects the secrecy and integrity of the ballots only during the transmission over the Internet. The ballots are not automatically protected on the client or server side. In fact, additional security technologies, mechanisms, and services are required to protect the secrecy and integrity of the ballots before and after they are transmitted over the Internet. There are additional risks for the secrecy of the ballots (i.e., privacy risks) related to the use of spyware (in the home setting) or remote system administration tools (in the institutional setting).

Due to the fact that a remote Internet voter uses his PC to cast a ballot and that this PC may be subject to malware, the insecurity of the client-side platform represents the major vulnerability (and Achilles heel) of remote Internet voting. Rivest coined the term secure platform problem to refer to the problem of protecting an inherently insecure client-side platform against malicious software and corresponding attacks [Riv01].

Due to the fact that the *secure platform problem* is hard and difficult to solve, there are several e-voting research and development projects that don't even address it. For example, in the FAQ document of the European CyberVote project[57], the question "Can a virus or Trojan horse attack CyberVote?" is answered in the following way:

"Yes, like any other client software in an insecure PC environment.

Anti-virus software should be used and strict security guidelines followed to limit the risk of a virus or Trojan horse attack.

Secure user interface techniques can be applied to the CyberVote client to prevent Trojan horses."

Unfortunately, the FAQ document does not further explain the term "secure user interface techniques." It turns out that there are not many security technologies, mechanisms, and services that can be used to effectively address the secure platform problem of remote Internet voting. In fact, we think that code voting as introduced next is one (if not the only) technology that may work in a real-world setting.

[57] http://www.eucybervote.org/faq_security.html#q35

3 Code Voting

The term *code voting* is used to refer to an e-voting technology in which the voter casts his ballot by providing a voting code instead of YES or NO (in the case of a vote) or a candidate's name (in the case of an election). The voting code, in turn, looks like a random string. If the alphabet consists of all decimal digits 0...9, then the voting code basically represents a number. In general, however, any alphabet can be used and the voting codes can be arbitrarily long.

To the best of our knowledge, the first code voting system was proposed by Chaum [Cha01]. In such a system, each voter is equipped with a code sheet (i.e., a sheet that itemizes all voting codes) and he must enter the appropriate voting codes to cast his ballot. An exemplary code sheet for an election is illustrated in Table 1. If the voter wants to vote for Bob, then he must enter 990234 (instead of "Bob").

Candidate	Voting code
Alice	236412
Bob	990234
Carol	141290
Dave	782755
Eve	774892
…	…

Table 1: A code sheet with voting codes

Due to the fact that voting codes look like random strings, code voting effectively protects against passive and active attacks:

- In a passive attack, the adversary sees a voting code sent over a network (using, for example, a network management or system administration tool), and must then be able to tell whether this code represents YES or NO (in the case of a vote) or to which candidate the code actually refers to (in the case of an election). If the voting codes are chosen with a good random bit generator or a cryptographically secure pseudorandom bit generator (PRBG), then the best the adversary can do is guessing. In this case, seeing the voting codes sent over the network does not help the adversary.

- In an active attack, the adversary does not only see a voting code sent over a network, but he can also manipulate it. For example, the adversary may employ malware or a client-side remote system administration tool to turn a voting code representing YES into a voting code representing NO (in the case of a vote) or a voting code of one candidate into a voting code of another candidate (in the case of an election). Again, if the voting codes are chosen with a good random bit generator or a cryptographically secure PRBG, then the adversary does not know the other voting codes, and hence the best he can do is again guessing.

In either case, the success probability of an adversary is not better than guessing, meaning that the best an adversary can do is guessing. This is indepedent from the adversary's computational resources and available time. Consequently, the security that is achieved is unconditional or information-theoretic. There are, however, two conditions that must be fulfilled to achieve this level of security:

- As mentioned before, the voting codes must be random, i.e., they must be chosen with a good random bit generator or a cryptographically secure PRBG;
- The code sheets must be personal and distributed out-of-band[58], using, for example, a trustworthy postal mail delivery service.

Also, it is important to note that code voting requires a modified voting behavior, and that there may be some legal constraints to consider (not addressed in this paper).

In spite of the fact that code voting as discussed so far is able to provide unconditional or information-theoretic security, it may still be the case that an (active) adversary simply deletes a voting code in transit. To protect against this attack, it may be worthwhile to have the server send back a verification code and have the voter verify this code.

Table 2 illustrates an exemplary code sheet with voting and verification codes. Again, if the voter wants to vote for Bob, then he must enter 990234 and wait for the server to send back the verification code 672345. If another verification code is sent back, then something illegitimate is going on and the voter is well advised to stop voting (needless to say that some dispute-resolving mechanisms must also be put in place here).

Candidate	Voting code	Verification code
Alice	236412	124355
Bob	990234	672345
Carol	141290	045686
Dave	782755	687432
Eve	774892	234115
…	…	…

Table 2: A code sheet with voting and verification codes

If the voter verifies the verification code, then it makes a lot of sense to communicate the result of the verification step to the server (otherwise, the server does not know whether the result is correct). This is where the confirmation code comes into place. Table 3 illustrates an exemplary code sheet with voting, verification, and confirmation codes. In our toy example, the voter would confirm the successful verification of the verification code 672345 by sending the confirmation code 574546 to the server. At this point, there is no need to continue the recursion (and send more codes back and forth).

[58] It is important that the code sheets must be provided outside the voter's PC (i.e., the PC that is used by the voter to cast his vote). If the code sheets were inside the PC, then malicious software could get and use them to change the ballots. Also, the voting codes must be randomly or pseudo-randomly chosen from a sufficiently large set of possible values to make the probability that malicious software can correctly guess them sufficiently small (i.e., negligible).

Candidate	Voting code	Verification code	Confirmation code
Alice	236412	124355	252435
Bob	990234	672345	574546
Carol	141290	045686	124145
Dave	782755	687432	243521
Eve	774892	234115	967468
…	…	…	…

Table 3: A code sheet with voting, verification, and confirmation codes

The bottom line is that there are many possibilities to implement code voting. In addition to casting a vote by simply entering a voting code, the voter may verify a verification code sent back from the server (to verify that he has casted the vote to an authentic server, and that the vote has been properly registered by the server). Also, the voter may acknowledge proper verification of the verification code by sending out a confirmation code.

In Table 4, we summarize the 2^3-1=7 possibilities to implement code voting. Among these possibilities, we think that the following four possibilities are meaningful in practice:

- Voting code-only implementation;
- Verification code-only implementation;
- Voting and verification code implementation;
- Full implementation (i.e., voting, verification, and confirmation codes).

Possibilities	Voting code	Verification code	Confirmation code
Voting code-only implementation	X		
Verification code-only implementation		X	
			X
Voting and verification code implementation	X	X	
	X		X
		X	X
Full implementation	X	X	X

Table 4: Possibilities to implement code voting

In a voting code-only implementation, the voter casts his ballot by simply sending a voting code to the server. In a verification code-only implementation, the voter casts his ballot as usual, but waits for a verification code sent back from the server. It is then up to the voter to verify this code. A verification code-only implementation is particularly interesting, because the voter has to minimally change his behaviour (i.e., he can still enter YES or NO and only validate the verification number sent back from the server). This advantage, however, may also be disadvantageous, because it is possible and likely that some voters don't care about the validity of verification codes sent back. As its name suggests, a voting and verification code implementation employs voting and verification codes. Last but not least, a full implementation employs voting, verification, and confirmation codes. It goes without saying that this is the preferred choice from a security viewpoint, and that all other choices represent tradeoffs.

A practically relevant question refers to the length of the various codes. Obviously, the length must make the probability to correctly guess a code sufficiently small. For example, if the number includes 10 binary digits (bits), then the probability of correctly guessing a code is $1/2^{10} = 1/1{,}024 = 0.000975562$. Due to the fact that the numbers cannot be verified off-line (without access to the code sheets), this seems to be sufficient. 10 bits can be represented with $\log 2^{10} = \log_{10} 1{,}024$ decimal digits which is slightly more than 3 digits. Consequently, 4 decimal digits can be used to encode a code and some redundancy to detect errors (error detection is particularly important for voting and confirmation codes that are entered by the user).

In theory, 10-bit code numbers can be randomly generated, using a random bit generator. In practice, however, the code numbers are more likely generated with an appropriately seeded pseudorandom bit generator (PRBG) or a construction that employs a keyed hash function, such as the HMAC construction [KBC97]. In either case, the generation of the code numbers is not further addressed in this paper.

Last but not least, we note that a guessing attack may have an equalizing effect on the outcome of an election or vote. If, for example, a candidate only gets a few votes under “normal” circumstances, then he may get an average number of votes under a guessing attack. This is because it is equally likely to guess a voting code for an unpopular candidate as it is to guess a voting code for a popular candidate. Hence, the outcome of an election or vote that is subject to a guessing attack may be equalized to some extent. Because we do not further address guessing attacks, this point is not further discussed in this paper.

4 CAPTCHA-based Code Voting

The potential difficulty of differentiating humans from computers pretending to be humans was addressed already in 1950, when Turing described his now-famous test. In short, the *Turing test* is a proposed test for a machine to demonstrate intelligence [Tur50]. It proceeds as follows: a human judge engages in a natural language conversation with one human and one machine, each of which are trying to appear human. If the judge cannot reliably tell which is which, then the machine is said to pass the Turing test. In order to keep the test setting simple and universal (to explicitly test the linguistic capability of the machine instead of its ability to render words into audio), the conversation is usually limited to a text-only channel such as a teletype machine as Turing suggested, or, more recently, Internet-based messaging.

In the mid-1990s, people came up with the idea of using a reverse Turing test to have a machine test whether a user is human. For example, in 1995, Lam of The Chinese University of Hong Kong implemented a reverse Turing test in a voting application written for Radio Television Hong Kong. The public was able to vote for their favourite singers and songs online for the first time in the annual "Top Ten Chinese Songs Award." To prevent automatic and machined submissions, users were required to correctly input a 6-digit number that was represented as an image. In 1996, the first reference of automated tests, which distinguish humans from computers for the purpose of controlling access to Web services, appeared in a manuscript of Naor [Nao96]. Other primitive reverse Turing tests seem to have been developed in 1997 at AltaVista to prevent bots from adding URLs to their search engine.

In 2000, von Ahn and Blum developed and publicized the notion of a *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA), which included any program that can distinguish humans from computers. They invented multiple examples of CAPTCHAs, including the first CAPTCHAs to be widely used on the Internet (at Yahoo!) [vABL04]. The acronym CAPTCHA is trademarked by Carnegie Mellon University. Alternatively, a CAPTCHA is sometimes called *Reverse Turing Test* (RTT) or *Human Interactive Proof* (HIP).

In general, there are many possibilities to implement CAPTCHAs, RTTs, or HIPs. A common type of (visual) CAPTCHAs requires that the user type in the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Such CAPTCHAs are also used in this paper (as an example). But there are many other visual CAPTCHAs and CAPTCHAs based on audio or video. More recently, for example, Microsoft Research has come up with a HIP called ASIRRA (Animal Species Image Recognition for Restricting Access) that works by asking users to distinguish between photographs of cats and dogs [E+07]. Audio CAPTCHAs, in turn, have been developed and are being deployed for handicapped persons. In essence, any task that can be efficiently solved by a human but is not known to be efficiently solvable by a machine can be turned into a CAPTCHA, RTT, or HIP. There are many opportunities for research and development here.

In CAPTCHA-based code voting, the voter does not cast his ballot directly by providing an appropriate voting code, but indirectly by clicking on an appropriate CAPTCHA. Clicking on a CAPTCHA, in turn, causes a random-looking voting code (representing a cryptographic hash value) to be sent from the browser to the server. Let us consider an exemplary (and simplified) election in Germany, in which the voter can select between five political parties. If, for example, a voter visits http://wahlen.nds.rub.de, then the voting server sends back a dynamically generated Web page in which the parties' acronyms are rendered as CAPTCHAs and visually presented to the voter in random order.

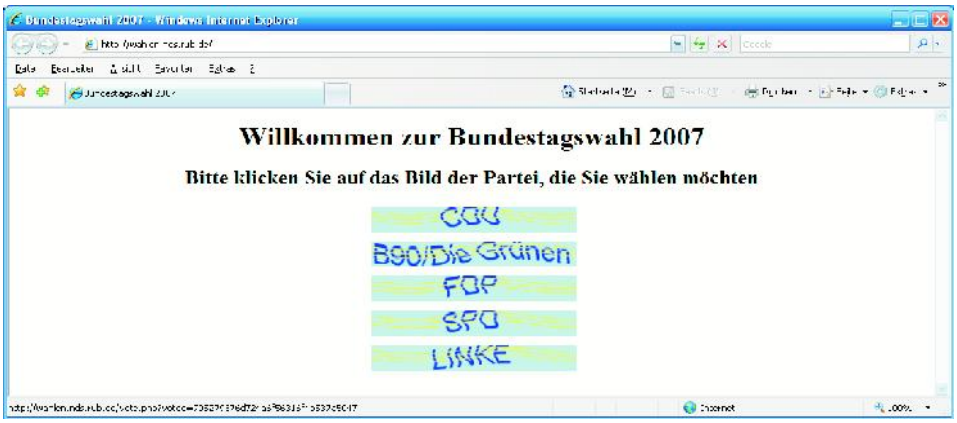


Figure 1: First screen for CAPTCHA-based code voting

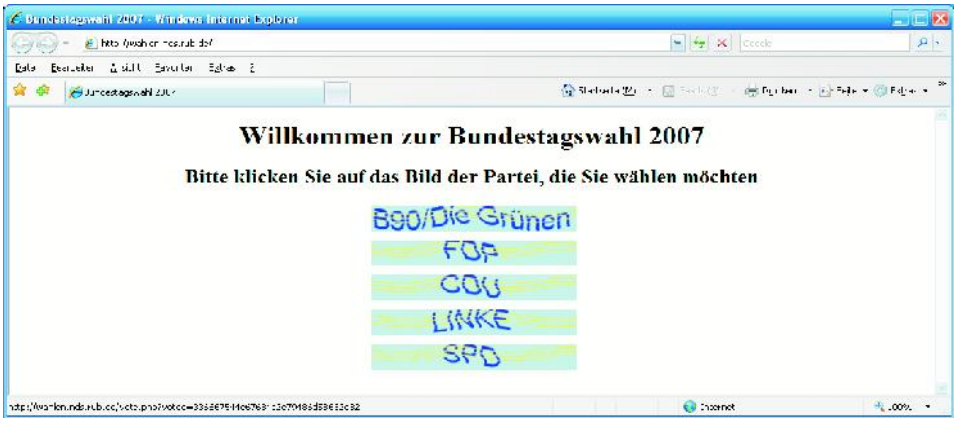


Figure 2: Second screen for CAPTCHA-based code voting

Figures 1 and 2 illustrate two possible screens. If, in this example, the voter selected CDU on the first screen (choice 1), then the voting code sent to the server would be:

705279376d724a6f56316f4b537a5047.

Similarly, if the voter selected CDU on the second screen (choice 3), then the voting code would be:

336667544e67684c2e79486d58632e32.

In either case, the voting code represents a cryptographic hash value and is visible in the browser's status line. Note that the two codes are different and unlinkable despite the fact that the selected party is the same. Also note that in CAPTCHA-based code voting, there is no urgent need to minimize the length of the voting code. The voting codes are sent by the browser to the server in a way that is transparent to the user, i.e., the user does not have to type it in. This simplifies things considerably, and the discussion held at the end of Section 3 is obsolete in this setting. So from a usability perspective, CAPTCHA-based code voting is perfectly fine. The user experience does not significantly deviate from what he knows and is accustomed to. In the following section, we address the question whether CAPTCHA-based code voting is also fine from a security perspective.

5 Preliminary Security Analysis

If one considers the use of code voting to overcome the secure platform problem, then one is mainly concerned with the possibility of automated client-side attacks mounted by malware. More specifically, one wants to make it impossible for an adversary to write malware that can modify a vote in some meaningful way. This must be true even if the malware has access to all information that is available in the client's operating system or browser. Note, for example, that such malware has access to the browser's state and content of Web pages, and hence that it is able to read out the voting codes. But it does not know what code belongs to what choice, and hence it can only make random guesses. In the example given above, the malware is likely to be able to read out the voting code 705279376d724a6f56316f4b537a5047 for the first choice on the first screen, but it is not able to associate this code to the CDU party (because this association is done outside the client system in the brain of the voter). Consequently, it cannot decide whether this selection is the appropriate one, and hence whether it should modify the vote. Also, in the case of an election with more than two options, if the malware knew that it should modify the vote, it would still not know which other option to select.

The bottom line is that CAPTCHA-based code voting remains secure (in the sense sketched above) as long as the CAPTCHAs in use remain secure, i.e., cannot be solved by a machine. If somebody can write a piece of software that can break the security of the CAPTCHAs, then this software can also be used to trivially break the security of CAPTCHA-based code voting. So we have to make the critical assumption that the CAPTCHAs in use are secure. This assumption is critical, because the security of CAPTCHAs has come under fire and many researchers are trying to compromise them.

Based on the assumption that the CAPTCHAs in use are secure, one can argue that CAPTCHA-based code voting remains secure as well. But there are still a few subtle attacks that must be considered with care. Let us briefly elaborate on two examples.

1. If an adversary has introduced himself in the communication channel between the client and the server, then he is representing a man-in-the-middle (MITM) and can display any CAPTCHA or CAPTCHA-like image. It is then simple for him to circumvent or bypass CAPTCHA-based code voting (because he can create the CAPTCHAs and therefore knows what they represent). Consequently, the use of technologies and mechanisms that protect against MITM attacks seems to be mandatory. There are a few such technologies and mechanisms available; examples include ciphersuites for the TLS protocol that support authentication based on pre-shared keys [BH06], SSL/TLS session-aware (TLS-SA) user authentication [OHB08], the use of client-side public key certificates, and a few more. Unfortunately, these technologies and mechanisms are not yet widely deployed, and hence, any currently available infrastructure for remote Internet voting and CAPTCHA-based code voting is vulnerable to MITM attacks. It is best to make this vulnerability explicit.

2. Since an increasingly large number of e-commerce application providers employ CAPTCHAs to make sure that their users are human, an adversary could collaborate with these providers to exploit the human resources (and capabilities) of their users. For example, an adversary could set up a free Web-based CAPTCHA service for e-commerce application providers. If invoked, this service could use CAPTCHAs found on compromised client systems and provide them to the users of the service. The responses could then be used by the malware to modify the vote in some meaningful way. In the example given above, the malware would input the five CAPTCHAs found on the first screen to the service. The service would dispatch the CAPTCHAs to individual users, and return the strings representing the names of the parties to the malware. The malware would then be able to decide if and how to meaningfully modify the vote. There is hardly anything that can be done technically to protect against such a distributed attack. Consequently, one must carefully monitor the CAPTCHAs that are used by service providers, especially during the time frames of the elections and votes that are supported by CAPTCHA-based code voting. Too many occurrences of strings that represent political parties or names of politicians should be taken as an alert.

We think that both attacks are relevant and must be considered with care. In particular, we think that the use of technologies and mechanisms to protect against MITM attacks and a careful monitoring of CAPTCHAs in widespread use are mandatory in a real-world deployment of CAPTCHA-based code voting.

6 Conclusions and Outlook

The secure platform problem is severe for remote Internet voting. The malware-based client-side attacks that are currently mounted against Internet banking (e.g., [ORH08]) can easily be turned into attacks against remote Internet voting. The attack vectors are essentially the same, i.e., it does not matter whether malware manipulates an Internet banking transaction or a remote Internet voting transaction. In either case, the manipulation occurs after user authentication and can be made transparent to the user. This should be kept in mind when people argue about the (in)security of remote Internet voting.

Against this background, we think that code voting provides an appropriate technology to address the secure platform problem of remote Internet voting, but that it is not particularly user-friendly. There are different possibilities to implement code voting, and these possibilities have specific advantages and disadvantages.

In this paper, we proposed the use of CAPTCHAs to improve the user-friendliness of code voting, briefly discussed the security of CAPTCHA-based code voting, and elaborated on a possible implementation. CAPTCHA-based code voting can only be as secure as the CAPTCHAs that are used. Alternatively speaking, if an adversary is able to break the CAPTCHAs in use, then he is also able to break the security of CAPTCHA-based code voting. Consequently, the current state-of-the-art in breaking CAPTCHAs should be closely monitored and observed. For example, there is a recently published low-cost attack on CAPTCHAs employed by Microsoft[59]. In spite of the progress that has been made in order to break the security of CAPTCHAs, we still think that CAPTCHA-based code voting provides an interesting possibility to implement code voting in a real-world setting, and that it has potential for the future. It is certainly worthwhile to implement it, and to explore its use (and usability) in a field study.

[59] http://homepages.cs.ncl.ac.uk/jeff.yan/msn.htm

References

[Ber08] Beroggi, G.: Secure and Easy Internet Voting. IEEE Computer, Vol. 41, Number 2, February 2008, pp. 52-56.

[BH06] Badra, M.; Hajjeh, I.: Key-Exchange Authentication Using Shared Secrets. IEEE Computer, Vol. 39, Number 3, March 2006, pp. 58-66.

[Cal00] California Secretary of State, California Internet Voting Task Force, Final Report, January 2000, http://www.ss.ca.gov/executive/ivote/.

[Cha01] Chaum, D.: SureVote: Technical Overview. Proceedings of the Workshop on Trustworthy Elections (WOTE '01), August 2001, http://www.vote.caltech.edu/ wote01/ pdfs/surevote.pdf.

[DR06] Dierks, T.; Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006.

[E+07] Elson, J. et al.: Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization. Proceedings of the 14th ACM Conference on Computer and Communications Security (ACM CCS 2007), 2007, http://research.microsoft.com/ asirra/papers/CCS2007. pdf.

[FKK96] Freier, A.O.; Karlton, P.; Kocher, P.C.: The SSL Protocol Version 3. Internet-Draft, 1996.

[Nao96] Naor, M.: Verification of a human in the loop or Identification via the Turing Test. 1996, citeseer.ist.psu.edu/naor96verification.html.

[OHB08] Oppliger, R.; Hauser, R.; Basin, D.: SSL/TLS Session-Aware User Authentication. IEEE Computer, Vol. 41, Number 3, March 2008, pp. 59-65.

[Opp02] Oppliger, R.: How to Address the Secure Platform Problem for Remote Internet Voting. Proceedings of the 5th Conference on "Sicherheit in Informationssystemen" (SIS 2002)}, Vienna (Austria), October 3-4, 2002, vdf Hochschulverlag, pp. 153-173.

[ORH08] Oppliger, R.; Rytz, R.; Holderegger, T.: Internet BankingClient-Side Attacks and Countermeasures. Submitted for publication.

[Riv01] Rivest, R.L.: Electronic Voting. Proceedings of Financial Cryptography '01, February 2001, http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf.

[Rub01] Rubin, A.D.: Security Considerations for Remote Electronic Voting over the Internet. Proceedings of the 29th Research Conference on Communication, Information and Internet Policy (TPRC 2001), October 2001, http://avirubin.com/e-voting.security.html.

[Tur50] Turing, A.: Computing machinery and intelligence. Mind, Vol. LIX, No. 236, October 1950, pp. 433-460.

[vA+04] von Ahn, L. et al.: Telling Humans and Computers Apart Automatically-How Lazy Cryptographers Do AI. Communications of the ACM, Vol. 47, No. 2, February 2004, pp. 57-60.

[Yao82] Yao, A.C.: Potocols for Secure Computations. Proceedings of 23rd IEEE Symposium on Foundations of Computer Science, Chicago, Illinois, November 1982, pp. 160-164.

Session 8: Political Issues of E-Voting

E-Voting in Brazil – Reinforcing Institutions While Diminishing Citizenship

José Rodrigues Filho

Universidade Federal da Paraíba, Cidade Universitária
58.059-900 João Pessoa, Brazil
jrodrigues-filho@uol.com.br

Abstract: Brazil became the first country in the world to conduct a large-scale national election using e-voting technology. What does it mean for democracy to hold an electronic election for millions of poor people, most of them living under the poverty line? Is the high investment in e-voting technologies designed to the benefit of millions of illiterate people? The discussions about the lack of security of e-voting in Brazil and in many other countries are based on a rather reductionist view that neglects both its social and political aspects. In this work, an attempt is made to expand the critique of the problems of e-voting beyond its lack of security and technological failures. It is argued that information technology in many parts of the world is reinforcing institutions and has done little to change our democracy. In its current form, e-voting technology in Brazil seems to be reinforcing some institutions while diminishing citizenship and democracy.

1 Introduction

There are numerous and conflicting interpretations in the concept of citizenship, but it is commonly understood in terms of a framework of rights and obligations [Ja98]. In many countries there are some core political rights and obligations normally associated with citizenship – voting, deliberation or participation in the political process, and the access or right to the provision of information. So, how to improve citizenship and political practices envisaged in these core political rights and obligations?

It is argued that while Information and Communication Technologies (ICTs) hold the potential to improve the democratic process, expand citizenship and empower the people, they have the ability to perpetuate or exacerbate existing inequalities and other divides. Commenting on the gap in access to ICTs, some authors have stated that "the information revolution could paradoxically become a cause of even greater inequality and worsening poverty" among developing countries [McO04]. In addition, there are comments about the dangers of digital opportunities pointing out that the "unequal diffusion of technology is likely to reinforce economic and social inequalities leading to a further weakening of social bonds and cultural cohesion" [UN05].

Little research has been conducted to answer questions related to the effects of ICTs on citizenship, the political process, and its opportunities and dangers. In addition, the literature has shown that answers to these questions have been rather extreme. They have either a sceptical view over-emphasizing the negative aspects of ICT, on the one hand, or, on the other hand, an optimistic or Utopian view, enthusiastically spelling out hope that new technologies would strengthen and enhance the democratic process [GI01].

It is stated that the influential political science research in modern democracy has narrowed citizenship and reduced it down to the right to vote in elections, turning democracy to be experienced at elections time and not between elections. In Brazil, voting is mandatory and the duty to vote is very much questioned by voters. E-Voting, as a political tool, was introduced as part of an electoral reform that seems to be reinforcing this very narrow concept of citizenship, especially taking into consideration that election turnout decreased in the last election and vote buying increased considerably. It seems that with the erosion of democracy, voter turnouts have declined in many countries, independent of the nature of voting as a right or as a duty.

There is a need of more empirical research surrounding citizenship and new technologies and not just theoretical discussions. Because Brazil was the first country in the world to conduct the biggest election in the planet using e-voting technologies, when more than 100 million voters cast their ballots on more than 406.000 touch-screen machines scattered all over the biggest country in South America, an attempt is made in this study to approach the topic of e-voting in the Brazilian citizenship subject, looking at the impact of the electoral reform (e-voting) on the realization of citizenship that should seek to empower people through the use of ICT. An electoral reform or a new technology may have a positive impact on democracy and citizenship, if developed and implemented from below and not from the top-down model of politics.

2 ICT and Citizenship

There are diverse understandings of the term citizenship, which require a broad range of philosophical, sociological and political theory for its discussions and debate. In a less narrow view, citizenships consist of a compact of legal rights, protections and duties between government and individual members of society. In a broad sense, citizenship represents a framework of universal political, civil, social and participation rights. According to Janowski, citizenship comprises active and passive rights and obligations. “Citizenship is passive and active membership of individuals in a nation-state with certain universalistic rights and obligations at a specified level of equality” [Ja98]. In short, there is no universal definition of citizenship, and it is a contested concept with multiple definitions. Citizenship is “a peculiar and slippery concept with a long history [Ri92].”

According to Elliot (2000), two different theoretical perspectives to access the roles of individuals and their interrelationships in the current debate of citizenship have been identified: traditional social liberal, and neo-liberal. The traditional social liberal approach, in which the Marshallian theory of citizenship have been extensively discussed for half a century, emphasizes the importance of civil, political and social rights as elements of citizenship [El00].

The neo-liberal approach, on the other hand, rejects the welfare state, as the social rights element of citizenship, and supports the free market. In short, it emphasizes individual obligation and denies the collective rights and responsibilities. Due to new relations between nation states and citizenship and democratic control, there has been reformulation of those traditional concepts of citizenship. Therefore, new notions of citizenship have come onto the recent academic agenda as follow:

• ecological citizenship concerned with the rights and responsibilities of the earth citizen [St94];

• cultural citizenship involving the right to cultural participation [Tu93];

• minority citizenship involving the rights to enter a society and to remain within it [El00]];

• cosmopolitan citizenship concerned with how people may develop an orientation to many other citizens, societies and cultures across the globe [He95].

• technological citizenship is concerned with the ways in which citizenship norms, rights, obligations and practices are encoded in the design and structure of our increasingly digital surroundings [Lo05].

The expansion of Information and Communication Technologies (ICTs) in several countries has given rise to many e-government and e-democracy systems and initiatives very much based on an administrative-technological perspective. The information technological network infrastructure created from a nation-state perspective or from above is oriented more towards the provision of services into a network than towards the implementation and development of democracy or citizenship. It is recognized how crucial these services are, but in many instances they do not actually empower the citizen. The establishment of e-government and e-democracy, and the implications behind the initiatives of the cyber-state, promise to revolutionize many countries in terms of governance and democracy. However, it is mentioned that “while there is the political possibility of shaping the emerging cyber-state as a vehicle of empowerment,” especially for the marginalized others, “there is also the prospect that Internet-facilitated government will exacerbate inequalities” and diminish citizenship status [Mc04].

Under this nation-state perspective or top-down model, citizenship is constructed based on principles of the liberal tradition and "citizenship rights are being reconceptualized to reflect the neo-liberal agenda, in which citizens are expected to take care of themselves and those who fail to become self-sufficient are considered problematic and deviant" [Mc04]. In this case, an alternative society is a self-help society, based on morals of helping that can produce community services by voluntary work. In consequence, a so-called 'new lower class' is emerging, even in the richest OECD-countries. "These people are the long-term unemployed, permanently poor, badly-off ethnic groups and those who have fallen through all social safety nets." In short, they are second class citizens that cannot realize the principles of good citizenship – autonomy, self-esteem, participation and influencing in their own reference community and society, challenging the traditional concept of citizenship.

With the expansion of ICTs there is a need to understand not only the opportunities created by new technologies but also the risks regarding the realization of citizenship and civil rights. Therefore, ICT and citizenship should not be separated, because ICT in itself does not guarantee the realization of the rights of the citizen. Despite the determinist view and the expanding literature favouring the use of ICTs in the information society, e-government and e-democracy, it is recognized that the citizenship is at risk. The problem is that the conditions of technology are emphasized, but it is not fully clear what exactly is meant by the concept of the citizens' information society. It is recognized that many initiatives are necessary to turn computers and the Internet into a tool for civic participation. If, in the developed world, it is found that "mere presence of favourable conditions for making ICT a civic tool are not enough" [Ol06], in developing countries the situation is too complex.

Unfortunately, in the developed world, most of the academic work produced does not seem to worry about the relationship between ICT and citizenship, making it difficult for people to believe that they make a difference in a local/national governing, because the agenda seems to be already set. On the other hand, in developing countries, in some instances, one may even fear making a critique on how badly resources are allocated in the field of information technology.

In a framework of citizenship rights and obligations comprising civil, political, social, and participation rights and obligations, underpinned by elements of 'good society,' such as freedom, equality and justice, the political rights and obligations of voting, participation in the democratic process and access to information were selected for further discussion. In short, what is the impact of the electoral reform that introduced e-voting technology in Brazil on the political rights and obligations normally associated with citizenship - voting, participation in the democratic process, and access to information?

3 E-Voting in Brazil

It is stated that both democracy and voting are processes much more complex than their electronic version and a secure voting system in itself is a basic element of a true democracy. The e-voting technology in Brazil consists of the so-called Direct Recording Electronic (DRE) devices, which allow voters to cast their ballots directly through touch-screen voting machines. In this case, voters have to go to the polling stations to cast their ballots after a conventional identification. In remote electronic voting systems voters cast their ballots remotely, using the full potential of ICT [RRB05]. In other words, the DRE is a kind of offline voting system and the Internet is the online voting system.

The modality of electronic voting in Brazil through machines of the type Direct Recording Electronic (DRE) Voting System or electronic ballot boxes (Urnas Eletrônicas - UR) does not seem to have modified the traditional ritual of elections. The great difference is that in the traditional voting system the voters could see the ballot papers fall into an urn bag, placed in it by themselves, surrounded by inspectors. With the electronic ballot box, the voters do not have the certainty that their votes were registered and no inspector or witness certifies this: the vote is registered electronically.

Therefore, in the current system of electronic voting (DRE), the voter does not see the ballot box, but a representation of it. In turn, the machine does not supply an independent and true registration of each individual vote that could be used for a count or verification of errors in the machine or some type of tampering. In this case, if the machine registers a result in its memory that is different from that chosen by the voter, neither the voter nor the inspectors will know about it. Because of this, some specialists in computer security believe that such machines are more vulnerable to tampering than any other form of voting system, especially through the use of malicious computer codes.

Some specialists argue that software can be modified in such a way that the results of an election can be modified, being very difficult to be detected [Fi03]. Consequently, the security of electronic voting is susceptible to failures and frauds and some Brazilian experts question our e-voting system and its security through Internet journals, forums, articles and books [BC06, Ma02, Si02]. Similarly, comments and reports of international scientists corroborate with what our academics and scientists say, such as reports that argue on the security and risks of this kind of system in the United States [BC06, CMIT01, Ko03, Ko03]. It is known that electronic voting has existed for a long time in developed countries such as the United States, Germany and Japan, among others [Ma00], but more recently there have been many concerns about e-voting insecurity, especially in the more traditional democracies.

Some authors have been in favour of a more reliable e-voting system that can have the so-called voter-verifiable trails and an open source code, and it is likely that this kind of system may appear with the advance of technology and its lower price, although it is alleged that e-voting will never be error-free. On the other hand, some authors have emphasized the importance of political and socio-technical approaches for the development of an e-voting system that can ensure public trust in the results of an election [RR05]. Thus, apart from the technical aspects, it has been mentioned already that e-voting in Brazil has exacerbated alienation and the digital divide [RG08].

Paradoxically, the Superior Electoral Court (Tribunal Superior Electoral – TSE), known as the Electoral Justice, is responsible for election administration in Brazil; it has unexpectedly and rapidly adopted one technological system that has not yet been sufficiently tested even in the developed world. According to the critics of electronic voting, the Electoral Justice has opened the doors for new and sophisticated frauds much more serious than the traditional ones [Ma05], once the ballot's verification became private and the Electoral Justice the owner of the ballot boxes [Fr02].

During the last ten years, the Electoral Justice in Brazil has developed an intensive campaign emphasizing the security of e-voting, and on how the citizens should be proud of this technology that is said to be made in Brazil. Consequently, through the use of an intense propaganda, the Electoral Justice was able to institutionalize e-voting, and most of the population is proud of e-voting machines, believing that they are more secure than the traditional system.

However, over the last few years, the complaints about e-voting machine failures, corruption, and all sort of other critiques have intensified both in Brazil and in other countries that held elections more recently, such as the United States, Holland and France. Early in 2007, for the first time, the Brazilian Congress created a Sub-Commission for Electronic Voting that opened some hearings to improve the security of e-voting in the country. In one of its first hearings, a famous Brazilian politician and one of the richest men in the country, confirmed that for several times, at election time, he was asked whether he would really want to be elected. In another hearing an expert in e-voting technology security stated that he trusted the banking system more than e-voting machines in Brazil. In other words, he stated that e-voting machines are not secure at all.

A few months latter the Sub-Commission for Electronic Voting recognized the e-voting system insecurity in Brazil and proposed e-voting machines with paper trail capabilities to enable voter verification during elections. Although the so called voter-verified paper trail is demanded as the essential requirement to mitigate the risks associated with software and hardware flaws, there have been questions as to whether voter-verified paper trails will provide a significant benefit, given the costs added to e-voting tools. It has been recognized that many of the problems associated with e-voting machines are caused by a lack of training for workers who sometimes do not even know how to change the paper in the machines with paper trail or administrative mistakes. Anyway, in the case of Brazil, a few hours after the Sub-Commission published its final report, the Electoral Justice in Brazil rebutted it.

4 Corruption, Vote Buying and Turnouts

One of the purposes to use e-voting technology in the developed world is to increase turnouts, due to the discredit of voters with politicians and political parties. So, the kind of electoral reforms proposed in many countries to make it easier for registered voters to cast their ballots tends to benefit politicians and their parties with perverse consequences towards political engagement [Be05].

In Brazil, many electoral reforms have been approved over the last few years, but none of them aiming at improving political engagement. Although we do not know about the true relationship between e-voting technology and turnout, during the last election turnouts have decreased in the Parliament election in Brazil. A decrease in turnout may be a reduction in citizenship, but its relationship with e-voting technology is not clear. In the last election there was an intensive campaign on the Internet from the young people proposing to make the vote null. How far this campaign has influenced the population is also not yet known.

It is necessary to make it clear that an increase in turnouts does not necessarily mean more political participation and civic engagement. In many countries there is some political participation at election time, but people need democracy between elections and not only at election time. People want to participate in the decision making process between elections, and this is not always the case. It is here that the use of ICTs may help voters to have a better engagement in the political process. In the case of Brazil, voters need government "of, by, and for the people."

What is e-voting for, when money is choking our democracy to death? With the increase in the cost of getting elected, exploding beyond the reach of ordinary people, during the last election it was possible to register that our representatives in the Brazilian Parliament are richer than their predecessors. In this case, is the Brazilian Congress, the so called "People's House," really the place for the highest bidder, considering that some of our representatives are elected based on an empire of corruption, turning elections on auctions?

It is known that corruption in elections in Brazil and in many other countries is not an abstract thing. It is a crude and disgraceful reality. Electoral corruption is a kind of arrangement usually involving candidates, donors and voters who are bribed to sell their votes in a transaction in which the object can be cash, food, cloth, construction material, medicine, and the provision of other services. Since the year 2000, the NGO named "Transparência Brasil" has carried out surveys about vote buying in Brazil. According to the Transparência Brasil, the Electoral Justice in the country is responsible for neglecting the problem of vote buying [TB06]. It is very strange that the Electoral Justice is very much in favour of the e-voting technology system used in Brazil and is enable to enforce the law to combat vote buying. Is there a need of e-voting technology for the elections of corrupted politicians? Vote buying by itself is a sign of reduced citizenship.

So, e-voting in Brazil has not stopped vote buying which is increasing, and in 2006, during the last election, was twice as high than in the previous elections. What is surprising is that vote buying is higher among persons with secondary or higher education than voters with only primary education or below. It is expected that the poorer the voters, the more vulnerable they are to offers. The surveys from Transparência Brasil have shown that this is not true. More offers were made to the poorer, but vote buying is registered among the wealthier classes [TB06]. In order to give an idea of the magnitude of the problem of vote buying in Brazil, in 2006 it was found that about 8% of voters were asked to sell their votes for money [TB06]. Considering the number of voters in 2006, this corresponded to about 8.3 million voters, and represents more than the population in some European countries and in some Brazilian states.

5 Conclusion

Because voting is mandatory in Brazil, there is a need of a democratic tool for civic and effective participation in the democratic process, which is contingent upon political participation. Democracy means widespread involvement of ordinary people in matters of governance. In its current trend, e-voting technology does not seem especially hopeful. For those who endorse technologies enthusiastically as they emerge, such as e-voting, any criticisms or requests for wider debate about policy options in technology are often regarded as negative and unhelpful. Critical voices have often been labelled backward and obstructive, especially when they try to explore social and political consequences of technological choices.

Some electoral reforms may have perverse consequences on citizenship and democracy. By making it easier for all citizens to vote does not mean improvement in democracy and citizenship, especially when a top-down political tool is designed in ways that bring more power to the political elite. Can we combine an approach very much based on market-driven forces (e-voting) that suits existing political and bureaucratic elites with a real process of democratization (e-democracy)? In other words, can the state provide services to please the citizens without democratic engagement?

There is no doubt that e-voting facilitates the work of the Electoral Justice in Brazil when, a few hours after an election, the names of those elected are informed. This brings prestige to the Electoral Justice whose power is reinforced by e-voting technology. Over the last ten years there has been an official massive propaganda in Brazil about e-voting and its security, in addition to training and demos on how to vote electronically. As a consequence, the majority of the Brazilian society trusts our e-voting system and its security. In this situation, it is quite hard to comment against e-voting in the country.

In spite of this, it seems that democracy in Brazil is at risk: women's representation in the Brazilian parliament has decreased; our representatives in the Parliament are getting richer than their predecessors, and richer politicians get richer after their elections; turnouts decreased in the last election, and vote buying increased substantially. Corruption in the Brazilian Parliament has reached such a level that a recent edition of the Economist has made reference to it as a "Parliament or Pigsty?" thus, commenting on the sophisticated criminal organization to buy votes [Ec07].

The political elite has no interest in discussing e-voting in Brazil, let alone the poor that are excluded completely from the political life. However, if political participation and civic engagement do not improve, there are substantial arguments to discuss e-voting in Brazil. Due to the trust in the system and the official voice supporting it, there is no chance to question the technology just in terms of its security. However, when social and political issues are questioned, there are many things that people have not thought of, and it is time to start arguing about it. If people care about citizenship, the time is appropriate for the debate about the relationship between e-voting technology and citizenship.

How helpful would it be if the academic research work in the developed world could look not only at the technicalities of e-voting, but to its social and political issues and on how it should be designed in ways to reflect our best understanding of freedom, social justice and addressing the source of inequality and injustice. The technical problems of e-voting, especially in terms of security, can be solved in the near future, and people can easily understand it. However, when matters related to social and political problems are considered, it will take years for the poor voters, for example, to understand what is going to happen to them. This situation forces us to care about them and the future of democracy. We cannot survive without the help of technology, but we cannot let the market work and express our politics just by watching the TV screen.

The e-voting project in Brazil is an initiative that merely reproduces traditional and dominant forms by which power is exercised. This is a tool that exacerbates inequality, alienation, and exclusion, but it seems that it is not awakening the "consciousness of how men are deceived in a permanent way."

References

[Ba05] Berinsky, A. The Perverse Consequences of Electoral Reform in the United States. American Politics Research, 33(4):471-491, 2005.

[BC06] Brunazo Filho, A.; Cortiz, Maria Aparecida. Fraudes e Defesas no Voto Eletrônico. São Paulo, All-Print Editora, 2006.

[BC06] The Brennan Center of the NYU School of Law. Brennan Center, New York, 2006.

[CMIT01] The Caltech/MIT Voting Technology Project. Residual Votes Attributable to Technology – An Assessment of the Reliability of Existing Voting Equipment (2001). Available: http://www.vote.caltech.edu/Reports/index.html.

[Ec07] The Economist. Parliament or pigsty? (2007). Available: http://www.economist.com/world/la/displaystory.cfm?story_id=8670490

[El00] Elliot, J. The Challenge of lifelong learning as a means of extending citizenship for women. Studies in the Education of Adults 32(1), 6-21, 2000.

[Fi03] Fischer, E.A. Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues, Congressional Research Service (CRS) Report for Congress, November, 4, 2003.

[Fr02] Freitas, Silvana de. Voto eletrônico amplia chance de fraude. Entrevista. Folha de São Paulo (2002). Available: http://www.brunazo.eng.br/voto-e/noticias/folha11.htm

[Gi01] Gimmler, A. Delibarative democracy, the public sphere and the internet. Philosophy and Social Criticism 7(4):21-39, 2001.

[He95] Held, D. . Democracy and the Global Order. Cambridge: Polity Press, 1995.

[Ja98] Janoski, T. Citizenship and Civil Society. Cambrige. Cambridge University Press, 1998.

[Ko03] Kohno, T et al. Analysis of the Electronic Voting System. John Hopkins Information Security Institute. Technical Report TR-2003-19, July 23.

[Ko03] Konrad, Rachel. E-Voting critics point to security hole. California primary results appeared online before polls closed. Associated Press MSNBC News (2003). Available: http://stacks.msnbc.com/news/964736.asp?0dm=n15ot.

[Lo05] Longford, G.: Pedagogies of Digital Citizenship and the Politics of Code. Techné 9:1 Fall 2005.

[Ma02] Maneschy, Osvaldo et al. Burla Eletrônica. Rio de Janeiro: Fundação Alberto Pasqualini, (2002).

[Ma00] Maneschy, Osvaldo. Fraude eletrônica nas eleições (2000). Available: http://www1.jus.com.br/doutrina/.

[Mc04] McNutt, Kathleen. "Will e-Governance and e-Democracy Lead to e-Empowerment? Gendering the Cyber State." Federal Governance: A Graduate Journal of Theory and Politics. 4.1, 2004.

[McO00] McNamara, K., O'Brien, R. Access to Information and Communicatio8n for Sustainable Development Opportunities and Challenges for International Community-Recommendations of the Access Working Group. In GKP II Conference, Global Knowledge Partenership Secretariat. Luala Lumpur, Malaysia, 2000.

[Ol06] Olsson, T.: Appropriating civic information and communication technology: a critical study of Swedish ICT policy visions. New Media & Society, 18(4): 611-627, 2006.

[RG08] Rodrigues Filho, J., Natanael Pereira Gomes. E-Voting in Brazil – Exacerbating Alienation and the Digital Divide. In Mishra, Santap Sanhari. E-Democracy – Concepts and Practice. Índia, IFCAI Books, 2008.

[Ri92] Riley, D. Citizenship and the Welfare State. In: Allan, J., Braham, P. Lewis, P (eds). Political and Economic Forms of Modernity. Cambridge: Polity Press, 1992.

[RR05] Randell, Brian, Peter Y. A. Ryan. Voting Technologies and Trust (2005). Available: http://www.cs.ncl.ac.uk/research/pubs/trs/papers/911.pdf.

[RRB03] Riera, Andreu Jorba, Jose Antonio Ortega Ruiz, Paul Brown. Advanced Security to Enable Trustworthy Electronic Voting. ECEG Proceedings. 3rd European Conference on e-Government. Trinity College, Dublin, 2003.

[Si02] Silva, Mônica Correia da. Voto Eletrônico - É mais Seguro Votar Assim - Florianópolis. Editora Insular Ltda, 2002.

[St94] Steenberg, B. Van ed. The Condition of Citizenship. Sage Publications: London, 1994.

[TB06] Transparência Brasil. Compra de Votos nas Eleições de 2006, Corrupção e Desempenho Administrativo. 2006.

[Tu93] Turner, B.S. ed. Citizenship and Social Theory. Sage Pub.: London, 1993.

[UN05] UNPAN. UN Global E-Government Readiness Report – From E-Government to E-Inclusion. Division for Public Administration and Development Management. Department of Economic and Social Affairs. United Nation, New York, p.3 2005.

[YD97] Yuval-Davis, N. National Spaces and Collective Identities: Border, Boundaries, Citizenship and Gender Relations. Inaugural Lecture, University of Greenwich, 1997.

The Voting Processes in Digital Participative Budget: A Case Study

Gleison Pereira de Souza[1], Cristiano Maciel[2]

[1]Prefeitura Municipal de Belo Horizonte
Secritaria Municipal Adjunta de Tecnologie da Informação
Rua Goiás nº 58 Centro, Belo Horizonte, Minas Gerais, Brazil
gleison@pbh.gov.br

[2]Centro Universitário Augusto Motta
Av. Paris nº 72, Bonsucesso, Rio de Janeiro, Brazil
crismac@gmail.com

Abstract: The Participative Budget consists of a process in which citizens can directly participate in decision-making and regulation of public budget spending. The experience of the City of Belo Horizonte (Brazil) with the Participative Budget is a consolidated e-democratic process in the government and, most importantly, for the population. By exploring techniques provided by Information and Communication Technology, the Digital Participative Budget was introduced. Hence, a new question is posed: which methodology should be used for the computerization of this process and what would be the best suited interaction and communication resources for the e-democratic process? Such decisions will be discussed in this paper. This paper presents the experience of Belo Horizonte with the implementation of the Digital Participative Budget, from the very conception and implementation of the project up to the voting period as well as its current phase. Accordingly, this paper broaches the discussion of the conditions that led to the development of this project, the model adopted for the computerization of the process, the functionalities of the web system, and the data from the case studies developed in Belo Horizonte.

1 Introduction

The Participative Budget, or PB, consists of a process in which citizens can directly participate in decision-making and regulation of public budget spending. Participation becomes effective by means of public Participative Budget assemblies, generally implying presence, which assures all citizens an equal weight in the decision-making process, regardless of their affiliation to any type of organization and lacking any privileges.

This public policy of political participation is one of the dialogical instruments created to bring together citizen and public administration in the generation of public interest, creating new pathways for Representative Democracy. Voting does not suffice; one must also participate. It is also not enough to base general (public) decisions in technical theses. These are certainly important, but consensus reached by those directly concerned (whether individual citizens or the community) must always be a desideration of this new Public Administration tendency.

The experience of the City of Belo Horizonte (Minas Gerais, Brazil) with the Participative Budget began in 1993 and was a result of an institutional change seeking the creation of government spheres that would be closer to the citizens and better able to perceive/address the demands of the populace. Today, the Participative Budget is already a consolidated process in the government and, most importantly, for the population of Belo Horizonte. Since it was first established, almost one thousand public constructions have been initiated and delivered to the population, a fruit of the population's choice via Participative Budget.

In the year 2006, the municipal government reached a milestone regarding this policy, guided by the pursuit of increased political participation. By exploring techniques provided by Information and Communication Technology, the Digital Participative Budget was introduced. Hence a new question is posed: which methodology should be used for the computerization of this process and what would be the best suited interaction and communication resources for the e-democratic process? Such decisions will be discussed in this paper.

Consequently, this paper presents the experience of Belo Horizonte with the implementation of the Digital Participative Budget, from the very conception and implementation of the project up to the voting period as well as its current phase. Accordingly, this paper broaches the discussion of the conditions that led to the development of this project, the model adopted for the computerization of the process, the functionalities of the web system, and the data from the case studies developed in Belo Horizonte.

2 Democracy and the Internet

In democracy power can be exercised by many, it is the people's expectations that prevail in all political decisions. According to [Ca64], democratic political forms are grounded on the assumption that no man or limited group of men is wise enough or good enough to govern others without their consent. Inquiring into their preferences is an essential part of the democratic process. However, freedom of expression in democracy does not merely involve being able to express an opinion about predefined options. In order for it to be effective, it must allow people to articulate a discourse, outline proposals, discuss them and confront them with other proposals through public communication means.

There are several classifications for democracy. This paper considers three democracy models as proposed by [As01]: quick, strong and thin. These models are based on the roots of traditional democracy and are used as a bridge between profound democratic theory and its electronic manifestations. A synthesis and later discussion of the characteristics, legitimacy, citizen's role, politician's administrative style and use of ICT's by these models is presented in Table 1.

Democracy	Quick	Strong	Thin
Characteristic	empowers people	consensus	choice efficiency
Legitimacy	majority	public debate	government responsibility
Citizen's role	decision-maker	opinion-maker	Consumer
Administrative style	limited	interactive	Open
Focus on use of ICT	decision	discussion	Information

Table 1: Democracy Models [As01]

Similarly to quick democracy, strong democracy demands active citizens, but rather than speeding up the decision-making process, strong democracy favours a slow and far-reaching involvement of people in the discussion and deliberation processes, —a situation that can be achieved in several electronic forums. While quick democracy starts from the assumption that most citizens have a critical sense of a wide variety of complex issues involving society and that decisions can be defined by the majority, strong democracy favours the development of individuals through information, discussion and debate. The strong model means not only empowering people but also providing education for the understanding of society. When people discuss social issues, a platform of respect, trust, tolerance and openness is created, and these are the essential ingredients of strong democracy. Strong democracy is indicated to conceive an e-Democracy model.

Typically, the only institutionalized channels people have to dialogue with the Government are political and administrative paths - insufficient for a participative democracy - and direct people-citizen dialogue, which is facilitated by communication means capable of turning the transmission of messages into a bilateral process.

We can identify three problems regarding democracy and citizen participation on the Internet [Wo00], namely: 1) difficulty to integrate Internet and political debate and consequently turn away from the ongoing unanimity that prevents any critical reflection; 2) difficulty to actually enter the field of politics; and 3) improving Internet applications, considering that the technical revolution did not have the expected effect on society, which means that the techniques are not efficient enough. Nowadays, traditional development of online e-Democracy follows a relatively predictable model [UK02]: organizations offer information to start with, then they add services and then attempt to add 'interactive' tools.

In order to use ICT's to effect, an infrastructure is needed to allow interaction with and access to the citizens and supporting: organization and classification (information and service); safety and reliability (electronic voting); moderation, control, quality and response guarantee (electronic participation). Implementing ICT's in e-Voting [OV04] [UK02] involves offering an electronic service package such as online voting and registration, devoting careful attention to safety, reliability and scalability. Eletronic participation represents the use of ICTs in supporting the information, consultation and participation of citizens [LC07]. Using ICT's to open new communication channels is far more complex, since it requires new relationships to be developed between government, citizens and representatives.

Those relationships in the Brazilian Government, in order to encourage citizen participation in decision-making, have been done through the Participative Budget (PB). The following section discusses this topic.

2.1 Participative Budget

In the Brazilian government model, during the electoral process, politicians present a government project. In case the project foresees a democratic and popular management, it must compromise, among others, the popular participation in the quarrel and application of the public resources, in the clear of practical administrative, in the recovery of the excluded segments citizenship of the society, in the environment sustainable development, in the preservation and valuation of the cultural patrimony and in the construction of dignity and respect to the human rights of a city.

During the execution of such projects, a significant population participation becomes necessary in the elaboration and control of the municipal public budget to consolidate the Participative Budget (PB). PB has been implemented in Brazil since 1989 in cities compromised with democratic management. Today, it is a reality in more than 140 cities.

Cities execute different methodologies looking for real citizen participation. In a general manner, PB is composed by:

- Marketing: papers and posters in the cities inform the calendar and methodology of PB in the current year;

- Council Members: represents the participants of the PB in a region or thematic, elected in an established number by the cities;

- Municipal Assembly or Forum of the PB: is the great meeting of the population to elect and/or to install the new council members of the PB and to deliver to the government, the hierarchy of the workmanships and services demanded for the cities. It's also argued themes/demands and its priority criteria and has realized a rendering of accounts.

- Participative Budget Council (PBC): space of representation and negotiation, making it possible for the council members to intervene in the debate of the municipal budget.

- Council Forum: they are regional or thematic meetings for debate, subjects of general interest. The regiment of the City Council of the Participative Budget is also argued and approved.

Garcia, Pinto and Ferraz [GPF05] analyze three prototypical attempts to increase the participation of the people and propose to create a system, the e-PPB (Electronic Participatory Public Budgeting) that simulates what an executive assistant would do, if humanly feasible, that can be summarized into five tasks:

1. Identification

- read each suggestion

- emphasize the keywords in the message

2. Interpretation

- rephrase the suggestion using the vocabulary of a predefined ontology

- classify each suggestion in one of the known themes or create new themes to incorporated creative ideas

3. Clustering

- group similar suggestions and add statistical information to the classified themes

- create an executive summary to show to the "boss"

4. Analysis

- check if there has been any executive action that has already addressed any of the provided suggestions

5. Follow-up

- send a personalized acknowledgement message to all suggestion senders with a special status note to the ones for which a government action has already been started

- keep an eye on eventual government measures that directly or indirectly make suggestions. Again, he or she would send a message advertising the measure, mainly to the ones who sent suggestions asking for that type of measure.

These are mechanical tasks that request intelligence, mainly concerning text mining activities. Technology is ready. In accordance with the tasks cited above, the authors proposed a computational helper to assist executives in listening to people's suggestions.

Some of the current Brazilian experiences use TICs to innovate the PB, however, they make use of strategies such as e-mail and voting/polls [GMP05] [MNG05] not allowing the full use of the Internet technology, and the consequence is a lack of participation of the citizens in the democratic process. On the other hand, experiences with consultative and deliberative processes, engaging citizens by using a virtual community, are being investigated [MG07].

Belo Horizonte (MG) city [BE07], has a significant experience in PB and is discussed in the next section.

3 Participative Budget in Belo Horizonte

Since 1993, the Participative Budget in Belo Horizonte has functioned as an instrument to bridge the interests of the Public Administration and the population, especially in areas with the most urgent need for public constructions and/or services, and, of course, proceeded by city planning (a crucial moment of political participation).

The PB renders effective many democratic goals and is currently, in Belo Horizonte, a biannual process, containing many steps where the population may express its intentions and deliberate on government planning. This process is noticeable for combining the participation of grassroots associations with that of unconnected individual citizens, which ends up representing a much more elevated and significant number of participants.

In 2006, the City of Belo Horizonte made an innovative achievement in the country in the field of public policy for participative democracy. Besides the already consolidated presential PB, an internet-based consulting and voting system, entitled Digital Participative Budget – Digital PB, was available for the population. Using Communication and Information Technology, the voting population of Belo Horizonte may directly, individually and equally define the public construction work that should be executed by the City, thus effectively partaking in the allocation of public spending.

This initiative was aimed at promoting the expansion of political participation, introducing and publicizing the PB to segments that would normally not get involved in its processes, such as middle class and young sectors of the population, and moreover falling upon the promotion of digital inclusion using internet resources. The Digital PB takes place every two years.

It is worth noting that Belo Horizonte, capital of the state of Minas Gerais, is the fifth Brazilian metropolis in terms of population size, which is 2.3 million. The complexity of a process involving such a numerous population was a challenge for the municipal public administration.

For the implementation of this process it was necessary to conceive a web environment projected with user-friendly interaction and communication resources and to promote the migration of the system to the Internet, safeguarding the basic premises of the participative budget. These aspects are discussed below.

3.1 Digital PB

The conception of a system with Belo Horizonte's Digital PB complexity forced the establishment of a careful methodology, as presented, and the selection of communication resources that would provide more interaction with the citizens, who are the targeted public of the application. This environment is available on [Be07].

In this sense, the following interaction and communication resources, among others for supporting additional functionalities, were defined: videos, streaming, forums, chats, contact us, public work perspectives and photographs, flash animation, news articles, weekly newsletters, and voting ballots. In this session, some of these user interaction resources are commented and illustrated:

The **forum** makes citizen-City interaction possible, allowing for the exchange and sharing of ideas, compliments, suggestions and directions. The experience demonstrated that the forum was an interesting and important means for the citizen to defend and debate the public construction works being voted. Free chats with the population also took place, permitting an exchange of ideas in real time. The screen below, in Portuguese Language, displays the discussion forum developed.

Figure 1: Forum in Digital PB

The **photographs** and **know more** allow the citizen to develop a more detailed outlook of the public constructions being debated and the subsequent voting process in the Digital PB. The menu topic, **construction perspectives** is a space created to give a future view of the construction, thus showing the before and after. See below the interface that displays pictures of the construction works.

Figure 2: Pictures of the construction works in Digital PB

The **video and streaming (DMP)** resources available in the Digital PB allow a good level of interactivity, since they synchronize voice, image, and text resources in a single application, providing a complete and dynamic overview of the construction work, besides providing accessibility to people with special needs. Streaming is a technology that permits watching the video while it is still downloading.

The **flash animations** were developed as a simpler visualization option than the videos of the construction works, geared towards the computers that do not possess the necessary resources to access the DMP video.

The **newsletter** is an electronic bulletin, by means of which the City of Belo Horizonte would send, via emails to registered citizens, information about the running of the voting process, construction works, testimonials, etc,.

In the voting stage, the citizen only needed to type the name and number of his/her voter registration in the Digital PB in order to access the ballot, which contained the list of construction works for voting. The projected interface was based on the design of a printed voter registration, as can be seen in the image below.

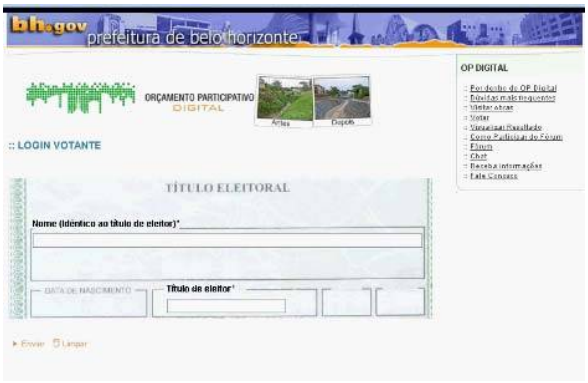


Figure 3: Ballot vote in Digital PB

This system was developed with state-of-the-art technology, with JAVA (J2EE) as the programming language, Oracle 10g as the database, web data security through HTTPS protocol, easy interactivity, accessibility and robustness.

With regards to system security, it is worth emphasizing that the captcha resource was used to avoid frauds (anti-robot function) in the voting screen, as well as a secure HTTPS system and certified digitals in the servers where the application was hosted.

3.2 Methodology implementation

The Digital PB project was divided in three moments: the pre-voting period, the voting period and the post-voting period, each one of them detailed below.

Pre-voting period

This period had three great marks, which are the selection of constructions that would be put to vote; the development of TIC tools and the establishment of partnerships; and publicizing the constructions to the population.

First of all, the government realized a pre-selection of 63 endeavors, seven in each one of the nine administrative districts in the city, according to criteria of social scope and relevance. After that, the COMFORCA (commissions formed by community leaders of each district, which follow and oversee the execution of the Participative Budget) were consulted for choosing 36 construction works, four per district, who would be submitted to vote. Contemplated in these constructions are the urbanization and renovation of avenues, construction/reform of leisure and cultural centers, and health center reforms, among others.

Correspondingly, partnerships were established for the project, among which began the partnership with the Regional Electoral Court. This Court provided the City with a database of all the voting population of Belo Horizonte. This database made it possible to create a solution based on the rule that limits voters to one single vote in each district, according to its voter registration; this provided more control, security and transparency to the voting process.

From the beginning of the second semester of 2006, the web system was developed for the publicizing and voting of the 36 pre-selected public construction works. By means of this system, the city's population could have access, in detail, to the information of 36 constructions, all of which have a great impact on Belo Horizonte; its responsibility is therefore to choose nine endeavors (one in each of the nine city districts) to be executed by the City.

Voting period

During the voting period, for those who did not possess Internet access, the City of Belo Horizonte installed 158 public and free voting stands in infocenters, schools and administrative agencies in all of the city's districts, with the presence of monitors to assist the citizen who was otherwise unfamiliar with the computer. Portable booths with various computers connected to the Internet were positioned in strategic places in the city during the voting period.

It is interesting to emphasize that the voting of Digital PB construction work gained so much ground that, in many locations, the community and companies installed, autonomously, voting stands; furthermore creating websites for publicizing and campaigning certain construction works, distribution of fliers in the streets, mobilizations, etc.

Simultaneously, the City launched a campaign on TV, Internet, radio, billboards, and bus advertisements in order to further stimulate political participation. Such parallel strategies are very important for the consolidation of the process. At the end of the voting process, the level of political participation in Belo Horizonte overcame the expectations, as can be seen by the data below:

- Number of voters – 172,938 (which corresponds to about 10% of the city's voting population).
- Number of votes – 503,266 (a citizen could vote up to nine times. The possibility of one vote for each district, with each district having four competing public constructions, was considered. Thus, each citizen could choose up to nine public works).
- Average votes per voter – 2.91 (the voters tended to vote more in the construction works of their region/district and less in other regions)
- Number of messages in the "Forum" – 912

- E-mails sent to “Contact Us” – 951

As a way to protect the transparency and control of the process, the individualization of votes was not held. Therefore, the profile of each elected person was not known and the vote was secret. It is important to emphasize that such information is part of the Regional Electoral Court´s database.

It is worthwhile listing the public constructions that won most votes in order to show their diversity:

- Barreiro Region – Implementation of a Sports Complex
- South-Center Region– Renovation of Praça Raul Soares (a square that holds a relevant historical significance for the city) and surroundings
- East Region – Renovation of the Medical Station
- Northeast Region – Linking the North and Northeast Regions (bridge construction and complementary construction)
- Northwest Region – Construction of a Hostel
- North Region – Construction of a Multiuse Cultural Center
- West Region – Implementation of a Medical Specialty Center
- Pampulha Region – Construction of an Ecological Park
- Venda Nova Region– Construction of an Ecological Park

Post-voting period

The nine endeavors chosen by the population of Belo Horizonte started to compose the City’s construction planning, and its execution estimated for the next two years.

The City Council of Belo Horizonte´s initiative of the Digital Participative Budget was approved by its government and population. In relation to the government, the General Auditor certified the reliability of the solution, ensuring transparency and security to citizens. The population met the administrative expectations, participating actively and taking the decision collectively. It is interesting to observe that the Digital PB stimulated the creation of collective and individual campaigns in favour of the works under discussion.

Data Access

Since the publication of the PB Digital website, 195,077 visits were registered up to the voting period, coming from 50 the countries highlighted in the map below, covering all five continents.

Figure 4: Countries that access the PB Digital

Fonte: *Google Analytics*. Acessado em 01/03/2008.

Surprisingly, access to the system exceeded the boundaries of Belo Horizonte. In Brazil, 24 out of 27 Brazilian states registered access. Other than Brazil, where the largest visitor concentration (193,527) logically occurred, the following visits were also registered: 1,077 from the United States, 126 from Portugal, 90 from France, 87 from Germany, 82 from Spain, among other countries. This shows that the experience of Belo Horizonte exceeds geographic limitations, generating worldwide interest in this political practice. The impact of this innovation can also be noticed by the various contacts and visits that the City has received from other cities and educational institutions that seek more detailed information about the Digital Participative Budget.

It is expected that this experience can serve as a trigger for other initiatives involving popular consulting initiatives in the sphere of Belo Horizonte. In this regard, the City Council of Belo Horizonte recently launched an Internet survey so as to collect the opinion of the city's inhabitants on whether shops should be open on Sundays and holidays. Participation in this survey was successful, despite being simple. Another aim is to contribute to the enhancement of discussions and to the implementation of concrete participative democracy practices in other governments.

The large participation registered in the first edition of the Digital PB brought a great challenge: how to expand even more the participation and discussion of the public construction work in the new edition, which will take place next November. For this new edition, citizens, instead of choosing a work in each region, will vote for only one, among the 10 largest investments demanded by the city. It is expected that the experience of the first Digital PB realized will allow this public policy of popular participation via Internet to acquire even greater relevance for people from Belo Horizonte and to become a common practice, as time goes by, in the interaction between Public Administration and citizens.

4 Conclusions

Due to the growing need to include every citizen in the digital world, it is advisable to map the languages used and accepted by the public in various means of communication, so as to improve interaction with the products offered by the government. The diagnosis of current participation initiatives and the citizens' true expectations converge on the need for an interactive environment. Digital inclusion will then be introduced in effect, considering not only the need for infrastructure but also facilitating active participation from citizens in the cyberspace. This paper discusses issues in the provision of e-Democracy, in particular in participative budget.

It is noticed that e-Democracy offers benefits for citizen and government alike. The citizens can assume a more active role in society, exercising their opinion power with ease and agility. Therefore, the digital revolution means more power for the people. For the government, unable as it is to turn its back on digital society, e-Democracy allows administration gains, transparency and more control over society through Internet-centralized data.

Using web-based Technologies and rendering possible a real citizen participation in the governmental questions is propitiating one Strong e-Democracy model with consensus, public debate, opinion-making, interactivity and discussion.

The participative budget proposal discussed here received the public administration's and population's approval. As for the government, the General Auditor guaranteed that it was trustworthy, attesting to its transparency and security. The population matched up to the administrative desiderate, participating actively and reaching a decision collectively. It is interesting to note that the Digital PB estimated the creation of collective and individual campaigns in favour of the works in debate. The strategies of winning voters for the preferred projects are varied, including the production of websites, advertisements and fliers, as well as face-to-face conversations in the streets.

A challenge of an e-participative environment such as this one is the extension of the scope of discussion. In this way, a good use of registered information, for instance, is in the forums, which could be better exploited since they contain additional information about community needs regarding the public works.

A user satisfaction study, by means of public research, will be conducted in view of offering improvements to the environment. Soon the next edition of the Digital PB will be initiated and will hopefully be as successful as this first version, increasing political participation in the definition of public policies in the municipal level.

Acknowledgements

We would like to express thanks to Marina Pombo de Oliveira and Vinicius Carvalho Pereira for the contributions regarding the translation of this paper.

References

[As01] Astrom, J. Should democracy online be quick, strong, or thin? Communications of the ACM 44,1, 2001, pg. 49-51.

[Be07] Belo Horizonte. OP Digital. Assessed in November 2007. Avaliable in http://opdigital.pbh.gov.br /in Portuguese/

[Ca64] Catlin, G.E.G. Tratado de Política. Rio de Janeiro: ZAHAR Editores. 1964. 489 p. /in Portuguese/

[GMP05] Garcia, A.C.B. Maciel, C.; Pinto, B.P. A Quality Inspection Method to Evaluate E-Government Sites. Electronic Government. In M.A. Wimmer et al. (Eds.): Proceedings of the International Conference on Electronic Government EGOV2005, 4, 2005, Copenhagem, Dinamarca. Lecture Notes in Computer Science, V. 3591, p. 198–209, Berlin Heidelberg: Springer-Verlag Ed., 2005.

[GPF05] Garcia, A. C. B.; Pinto, F.; Ferraz, I. N. Eletronic Participatory Budgeting (E-PPB): increasing people participation in the decision-making process. International Journal of Web Based Communities IJWBC, Inderscience, v.1, n. 4, p. 504-517, 2005.

[LC07] Lourenço, R. P.; Costa, J. P. Incorporating citizens' views in local policy decision making processes. Elsevier: Decision Support Systems 43, 4 (Aug. 2007), 1499-1511. 2007.

[MNG05] Maciel, C; Nogueira, J.L.T; Garcia, A.C.B. An X-Ray of the Brazilian e-Gov Web Sites. Human-Computer Interaction, INTERACT2005, 13, 2005, Rome, Italy. Lecture Notes in Computer Science, V. 3585, p. 1138 – 1141, 2005.

[MG07] Maciel, C., Garcia, A.C.B. Design and Metrics of a 'Democratic Citizenship Community' in Support of Deliberative Decision-Making. In M.A. Wimmer, H.J. Scholl and A. Grönlund (Eds.): Proceedings of the International Conference on Electronic Government, EGOV 2007, 6, Lecture Notes in Computer Science, V. 4656, pp. 388–400. Berlin Heidelberg: Springer-Verlag Ed., 2007.

[OV04] Oostveen, A; Van den Besselaar, P. From Small Scale to Large Scale User Participation: A Case Study of Partipatory Design in e-Government Systems. Proceedings Participatory Design Conference 2004. Toronto, Canada. ACM, 2004.

[PC05] Price, V., Cappella, J. Health care, i.t. and e-government: Constructing electronic interactions among citizens, issue publics, and elites: the healthcare dialogue project. ACM International Conference Proceeding Series; Vol. 89. pp. 139-140, 2005.

[UK02] UK. In the service of democracy, a consultation paper on a policy for eletronic democracy. Acesso em 22/02/2005. Available on http:://www.e-democracy.gov.uk/downloads. 2002.

[Wo00] Wolton, D. Internet: petit manuel de survie. CNRS/França. Paris, Flammarion, 2000.

Robert Krimmer, Rüdiger Grimm (Eds.)

Electronic Voting 2010 (EVOTE2010)

4th International Conference
Co-organized by
Council of Europe, Gesellschaft für Informatik
and E-Voting.CC

July 21st - 24th, 2010
in Castle Hofen, Bregenz, Austria

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-167

ISBN 978-3-88579-261-1
ISSN 1617-5468

Volume Editors
Mag. Robert Krimmer
E-Voting.CC gGmbH
Competence Center for Electronic Voting and Participation
Pyrkergasse 33/1/2, A-1190 Vienna, Austria
Email: r.krimmer@e-voting.cc
Prof. Dr. Rüdiger Grimm
Universität Koblenz-Landau
Institut für Wirtschafts- und Verwaltungsinformatik
Universitätsstraße 1, D-56016 Koblenz, Germany
Email: grimm@uni-koblenz.de

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

Castle Hofen has been the meeting place for e-voting specialists working in academia, administration, politics and industry since 2004. This interdisciplinary setting has brought many fruitful discussions and influenced the further development of the topic in many ways.

The continued interest is best reflected in the over 30 papers which we received following our call for papers. To make the conference again as attractive as in the past, we had to select the best papers for presentation based on a double blind review process.
Special thanks go to the Council of Europe and the working group ECOM - Ecommerce, E-Government and Security of the Gesellschaft for Informatik for their support in organizing this conference.

Further thanks go again to the Gesellschaft for Informatik and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Ministries for Science and Research (BMWF), for Interior (BMI), and the Regional Government of Vorarlberg for their continued support.
Without the help of the programme committee, who were always available with their advice, the conference would not have reached the level it has today.

Finally we would like to thank Thorbjørn Jagland, general secretary of the Council of Europe that the conference can take place under their auspices.

Vienna, Koblenz, July 2010 Robert Krimmer, Rüdiger Grimm

Co-Organizers

E-Voting.CC gGmbH
Competence Center for Electronic Voting and Participation

Council of Europe

Gesellschaft für Informatik
Working Group for E-Commerce, E-Government and Security

Introductory Words

The far-reaching changes made by the technological revolution help people to communicate instantly with others regardless of their respective locations. People travel around the globe more frequently and millions engage in social networks and use new forms of internet-based communication systems to share their thoughts and ideas. Electronics and social systems are blending into each other to create new communication channels.

These developments present democracy with an opportunity: information and communication tools can be used to foster greater participation in political processes, regardless of time and place. For example, using electronic voting systems to cast one's vote via the internet has become a real option.

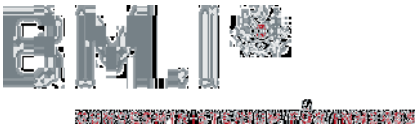
But what are the political implications of e-voting and what are the socio-cultural issues? What are the technical challenges and the limitations to e-voting systems? These are just some of the questions which need to be debated and answered.

International sharing of current research, standards and practices is vital if e-voting is to gain public confidence as a reliable and democratic voting tool. With this in mind, the Council of Europe welcomes the Fourth International Conference on Electronic Voting as a unique occasion for representatives of governments and international organisations, academia and businesses to exchange their views and expertise in the field of e-voting.

Thorbjørn Jagland
Secretary General of the Council of Europe

Supporters


BMWF
Bundesministerium für Wissenschaft und Forschung


BMLFUW


Vorarlberg
unser Land

Introductory Words

Dear Conference Participants,

This year is the fourth time that the renowned international EVOTE conference will take place in Austria, on the shores of the beautiful Lake Constance. Since 2004, when this biennial conference was held for the first time, much progress has been made all over the world in the field of electronic voting. In this respect, 2004 was a turning point in many ways: it was not only the birth of the EVOTE conference in Bregenz, Austria, it was also the year in which the Recommendation of the Committee of Ministers of the Council of Europe to Member States on Legal, Operational, and Technical Standards for E-voting was passed—and the Federal Ministry of the Interior published its first detailed report on the feasibility of e-voting.

However, six years is a long time in the world of technology. Modern citizens of today use computers and other means of modern communication in a much wider way than they did in 2004. The Internet as well as mobile phones and other handheld devices influence our daily lives in an unprecedented way. Austria is fully aware of this phenomenon and is internationally known as a forerunner in terms of e-government applications. My Ministry, being the competent administrative authority for electoral matters in Austria, has been very active in doing research in the area of e-voting for a number of years.

I consider it crucial to keep track of new technological developments in the field of democratic participation. Learning more about national and international experiences in e-voting, especially concerning remote Internet voting, is fruitful and essential for election officials, governments, policy makers, and legislators when discussing possible future solutions to make more people participate in elections and other instruments of direct democracy.

Elections in Austria enjoy the solid trust of society and have a high degree of transparency. It will be indispensable to keep these high standards when implementing new technologies in future elections. Finding the balance between accessibility, user-friendliness, and the highest degree of security in any kind of electronic voting system is the top challenge which has to be tackled. The secrecy of the vote, as an indispensable value in a free world, must never be compromised.

In a rapidly advancing field such as e-voting, new issues are constantly brought to the discussion table and require input from the "best of the best." The EVOTE2010 conference is the ideal forum for this task. E-voting experts from around the globe, both practitioners and representatives from academia, are gathered here and prove how much responsibility and credibility is attached to the discussions.
I wish this conference the very best, and I look forward to the results and products of the presentations and debates.

Dr. Maria Fekter
Federal Minister of the Interior

Sponsors

Bundesrechenzentrum GmbH, Austria

Micromata GmbH, Germany

Scytl, Spain

Programme Committee

- Mike Alvarez, USA
- Frank Bannister, Ireland
- Jordi Barrat, Spain
- Josh Benaloh, USA
- Nadja Braun, Switzerland
- Thomas Buchsbaum, Austria
- Chantal Enguehard, France
- Simon French, UK
- Thomas Grechenig, Austria
- Ruediger Grimm, Germany
- Thad Hall, USA
- Catsumi Imamura, Brasilia
- Norbert Kersting, South Africa
- Monique Leyenaar, Netherlands
- Robert Krimmer, Austria
- Laurence Monnoyer-Smith, France
- Hannu Nurmi, Finland
- Wolfgang Polasek, Austria
- Michael Remmert, France
- Peter Ryan, Luxembourg
- Josep Reniu, Spain
- David Rios, Spain
- Fabrizio Ruggeri, Italy
- Kazue Sako, Japan
- Berry Schoenmakers, Netherlands
- Robert Stein, Austria
- Dan Tokaji, USA
- Alexander Trechsel, Switzerland
- Melanie Volkamer, Germany
- Dan Wallach, USA
- Gregor Wenda, Austria

Organization Committee

- Daniel Botz
- Manuel Kripp
- Nicole Lundeen
- Gisela Traxler
- Felix Wendt

Content

Overview

Robert Krimmer[1], Rüdiger Grimm[2]

[1]E-Voting.CC gGmbH
Competence Center for Electronic Voting and Participation
Pyrkergasse 33/1/2, A-1190 Vienna, Austria
r.krimmer@e-voting.cc

[2]Universität Koblenz-Landau
Institute for Information Systems Research
Universitätsstraße 1, D-56016 Koblenz, Germany
grimm@uni-koblenz.de

This fourth proceedings volume of the EVOTE conference series features an impressive set of papers dealing with various aspects of electronic voting. It is the task of this conference series to enable the discourse amongst specialists working in academia, administration, politics and industry so that understanding, cooperation and future research can emerge. The conference includes discussions of practical work, its evaluation and theoretical foundation. In particular, it takes up the most urgent challenges that came up during the past two years. Therefore, special topics include end-to-end verifiability and certification of electronic voting systems. The papers are presented in the following.

The **first session** deals with the recent experiences made in the United States and Austria. First *Thad Hall, Charles Stewart, and R. Michael Alvarez* present the connex between voting technology and voter experience in the gubernational races in New Jersey and Virginia. Then *Robert Krimmer, Andreas Ehringfeld and Markus Traxl* present findings from the evaluation of the contested 2009 federation of students election, which offered electronic voting via the Internet for the first time in Austria. Thirdly the large and designated team consisting of *Alan Sherman, Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald Rivest, Emily Shen, Bimal Sinha, and Poorvi Vora* report from a mock election using an end-to-end verifiable electronic voting system.

In the **second session** the socio-cultural dimension of electronic voting is discussed. Here *Letizia Caporusso* discusses the role of trust, participation, and identity. Then *Philipp Richter* presents how the voter experience with Internet-based voting could be made as similar as voting in the polling station.

The **third topic** is dealing with certification and evaluation of electronic voting. Here *Rüdiger Grimm, Katharina Hupf, and Melanie Volkamer* start an extension of the formal model presented at EVOTE08. *Niels Menken* and *Kai Reinhard* show to which degree the remote e-voting system POLYAS is complaint with the common criteria protection profile. *Komminist Weldemariam* and *Adolfo Villafiorita* go on from there and present the current state in the development of e-voting systems.

Session four will host the presentation of *Axel Schmidt, Melanie Volkamer and Johannes Buchmann* on an evaluation approach for voting service providers.

In the **fifth session** *Rojan Gharadaghy and Melanie Volkamer* try to explain end-to-end verifiability to the non expert. In a different approach *Jordi Pujol-Ahulló, Roger Jardí-Cedó, Jordi Castellà-Roca* will classify these systems. Then *Stefan Popoveniuc and Andrew Regenscheid* will present a practical approach of a end-to-end-verifiable voting system.

In **session six** we will come back to e-voting experiences, where *Thad Hall and Leontine Loeber* will discuss the political environment and how it influences the discussion around e-voting. *Roberto Verzola* will show an innovative way on how to input voting results based on basic booking-keeping principles. *Andreas Ehringfeld, Larissa Naber, Thomas Grechenig, Robert Krimmer, Markus Traxl, and Gerald Fischer* discuss the Council of Europe Recommendation Rec(2004)11 how the experiences with the attacks on the federation of students‘ election in 2009 could be reflected.

In the **seventh session** e-voting protocols are discussed. Here *Jordi Puiggali and Sandra Guasch* present an universally verifiable efficient re-encryption mixnet. Then *Reto Koenig and Eric Dubuis* discuss how blind signature based internet voting systems can be made more secure using bulletin boards.

In the **final session** on theoretical and practical implications of e-voting *Oliver Spycher and Rolf Haenni* discuss how hybrid voting systems can be made coercion-resistant. *Masahiro Iwasaki* closes with a description of e-voting in Japan.

These papers give a good overview on the fast developments in the past two years. It also shows the necessity and importance of interdisciplinary research. Further we hope Castle Hofen will for long be home to these fruitful discussions.

Session 1: Recent Developments in E-Voting

Voting Technology and the Election Experience: The 2009 Gubernatorial Races in New Jersey and Virginia

Charles Stewart III[1], R. Michael Alvarez[2], Thad E. Hall[3]

[1]Kenan Sahin Distinguished Professor of Political Science,
Massachusetts Institute of Technology
77 Massachusetts Avenue
Room E53-470
Cambridge, MA 02139-4307 USA

[2]Professor of Political Science, California Institute of Technology
1200 E. California Blvd. MC 228-77
Pasadena, CA 91125 USA

[3]Associate Professor of Political Science, University of Utah
260 S. Central Campus Drive, Room 252
Salt Lake City, UT 84112 USA

Abstract: In this paper, we examine the attitudes of voters regarding the voting experience in the 2009 gubernatorial elections in New Jersey and Virginia. We focus especially on the way in which voting technology experiences that voters have had **affect** their confidence in the voting process, their attitudes toward fraud and reform, and other aspects of the voting process. We find that voters are sensitive to the voting mode they use—in person voting compared to absentee voting—as well as to whether they get to vote on the technology they prefer (paper versus electronic). Finally, the privacy that voters feel in the voting process is also important in shaping the voter's confidence.

1 Introduction

In the aftermath of the 2000 presidential election in the United States, groups like the Caltech/MIT Voting Technology Project (VTP) began studying the voting technology and the process of voting in American elections [VTP 2001].[1] Many of the early studies like the work of the VTP, though, focused either on survey data collected for other purposes (like the Census Bureau's Current Population Survey) or on the analysis of aggregated election returns [Al09]. These studies, while important, were unable to study in detail the voting experience --- and they were unable to relate the voting experience directly to the technology used by the voter to cast his or her ballot.

However, in recent years, the situation has changed, as detailed survey data on the voting experience has begun to be collected in earnest. In the 2007 gubernatorial elections in three states, in the Super Tuesday presidential primary races in 12 states, and then in the 2008 presidential election, the VTP conducted surveys in the appropriate states to determine the quality of the voting process across all modes of voting—early voting, absentee voting, and election day voting. The goal of these studies was to determine the way in which voters experienced the election process. In this paper, we use data from the most recent study by the VTP of voting experiences in New Jersey and Virginia in each state's 2009 gubernatorial elections. These studies built, in part, on earlier work designed to study the voting process as experienced by the voter. Scholars have studied the confidence of voters in the voting process [AH08; AHL08, AHL2009; AS05; BHC05], experience voters have had with their poll workers [HMP09; Ha09], and combinations of these experiences [AAH07; CMMP08]. However, most of these studies have been state-specific studies and many have focused on Election Day voting experiences, not considering the fastest growing part of the voting experience. These studies have also all focused on federal elections.

In this study, we consider a different type of American election, the off-year gubernatorial election. Five states have off-year gubernatorial elections; Virginia and New Jersey are on one cycle (e.g., 2009, 2005, 2001) and Kentucky, Louisiana, and Mississippi are on a different cycle (e.g., 2007, 2003, 1999). Our data analysis allows us to consider voter confidence in this slightly different context. In this study, we also specifically focus on how voters' experiences were affected by the voting technology they used to cast their ballots and the voting technology – paper or electronic – that is their preference.

[1] This paper uses data from the *2009 Survey of the Performance of American Elections*, which was funded by The Pew Charitable Trusts *Make Voting Work* Initiative. All findings are based on the analysis of the authors and do not reflect the views or opinions of the Pew Charitable Trusts.

2 Data and Analysis

The data in this analysis come from the *2009 Survey of the Performance of American Elections* (SPAE), and builds on the *2008 Survey of the Performance of American Elections,* which was the first nationwide effort to gauge the quality of the election experience from the perspective of voters [AAB09]. The data presented here come from the 2009 Survey of the Performance of American Elections (SPAE). The 2009 SPAE was an Internet survey that involved 1,200 interviews of registered voters in New Jersey and 1,300 interviews of registered voters in Virginia. The survey was in the field the week following the election, beginning Thursday, November 5 (two days after the election), with 98% of interviews completed by Monday, November 9. *YouGov/Polimetrix* conducted this survey entirely on the Internet using state-level matched random samples in each of the states. The respondents were recruited through a variety of techniques and the resulting sample matched the state populations on important demographic characteristics, such as education, income, race, and partisanship. The survey questionnaires were pilot tested in the November 2007 gubernatorial elections in Mississippi, Kentucky, and Louisiana and in the February 2008 Super Tuesday presidential primary. The main body of the survey asked a series of items about the experience of voters on Election Day, in early voting centers or during postal voting.

We checked the validity of the results by comparing the self-reported vote for governor in each state against the actual election returns. The results were very close and easily within sampling error.[2] We also compared some simple cross-tabulations within our survey with similar cross-tabulations from the network exit polls. We do not report those results here, but there is very close agreement between our results and the exit polls when we break the results down by sex, party, and reported 2008 presidential vote.[3]

3. Voting Experience

The voting experience is an important part of the democratic process. It is through voting that individuals express their preferences for policy, either through the election of representatives or directly through voting on referenda and initiatives [Pi67]. The act of voting has changed dramatically over the past 200 years [Be04; Ke00] and voters have certain expectations about the voting process, including about voter privacy and voting experiences [e.g., KMN10; GHD09]. We also know that variations in the voting experience can affect voter confidence and their attitudes about the voting experience. For example, voters who rate their poll worker-voter interaction higher are more likely to be confident that their votes were counted accurately [HMP09]. Likewise, we know that absentee voters are less confident that their votes are cast correctly compared to voters

[2] For example, in New Jersey the unofficial return results/survey results were Corzine (D) 44.4/42.1, Christie (R) 49.0/48.4, and Daggett (I) 5.7/8.6. In Virginia, the results were McDonnell (R) 58.6/59.4 and Deeds (D) 41.3/39.9.

[3] In the interest of brevity, we do not report standard errors in this paper. In general, in an analysis of 1,200 observations and a mean proportion at 50%, the 95% confidence interval is ±2.9%.

who vote in person in a precinct (either on election day or early) [AHL08]. We also know that problems at the polls – long lines, machine problems, and the like – all serve to lower evaluations of the voting experience at the polling place.

Our analysis here considers the voting experience in New Jersey and Virginia in November 2009 and focuses on the role that technology plays in the voting experience. We not only consider the role of voting technology, but also the use of electronic media prior to the election to learn more about the voting process. We start our discussion with this pre-election information search process and then consider the election process itself. We conclude by examining voter evaluations of election fraud.

	New Jersey	Virginia
Candidate position statements	74%	75%
News about the election	64%	62%
Polling place location	17%	23%
Sample ballots	15%	15%
Instructions on how to vote absentee	7%	8%
Instructions on how to vote at a polling place	5%	3%
Other	4%	5%

Table 1: Use of the Internet for Political Use

One critical part of the Internet and society is that individuals can now use the Internet to collect information about the voting process prior to voting. Voters can use the Internet to find out more about where they can vote, how to vote, and about the candidates for whom they can vote. Interestingly, we find that only 34% of respondents in New Jersey and 47% of those in Virginia reported that they had gone "online to find out information about the November 2009 election." In Table 1, when we examine the reasons why individuals visited the websites that they did, we find that most people used the Internet to find information about the candidates or track news about the election. Fewer than 1 in 5 respondents who went online did so to get information about their polling place, sample ballots, or information regarding how to vote. Respondents generally used the Internet for news about the election and the candidates, relying on the Internet only a little to understand the mechanics of voting.

Once voters get to the polling place, they may or may not have to wait in a line to vote. The 2008 SPAE found that African Americans wait in line to vote significantly longer than do Whites. For instance, in November 2008, African Americans waited twice as long to vote (27 minutes, on average) than did Whites (13 minutes). Although some of this difference may be attributed to the excitement generated by the Obama campaign

and a surge in African-American turnout in November 2008, examples of this pattern in other elections suggests the need for a richer explanation of this pattern. One important explanation may be that some individuals arrive at the polls before they open, or there is a clustering of voting at specific times.

We find that time of voting does explain some of the wait time problem. African Americans did report waiting longer to vote in both New Jersey and Virginia. In New Jersey, the estimated average wait was 1.7 minutes for Whites and 3.2 minutes for Blacks; in Virginia, the averages were 2.8 and 8.2 minutes, respectively. However, when we exclude early-arrivers (people who arrive before the polls are open) from the calculations, average wait times in Virginia were 2.7 minutes for Whites and 6.4 minutes for Blacks. The racial disparity remains, but it has been reduced. The racial differences are also explained by the fact that African Americans are more likely to live in large cities where lines are longer, regardless of race, compared to smaller towns and suburbs. Even so, *within community types,* African Americans still waited longer. For instance, within big cities, African Americans reported waiting 11 minutes to vote, compared to 5.9 minutes for Whites; within the outer suburbs, the reported waits were 3.4 minutes for Blacks and 2.0 minutes for Whites.

		Precinct Voting Technology			
		New Jersey		Virginia	
		DRE	DRE	OPSCAN	MIXED
No Line	N	660	372	170	103
	Percent	70.66%	62.42%	68.55%	68.67%
Less than 10 Min Line	N	247	185	59	40
	Percent	26.45%	31.04%	23.79%	26.67%
10- 30 Min Line	N	24	29	13	6
	Percent	2.57%	4.87%	5.24%	4.00%
30 or More Line	N	3	10	6	1
	Percent	0.32%	1.68%	2.42%	0.67%

Table 2: Lines and Voting Technology

When we consider line length and voting technologies, we see that, in Virginia, voters were more likely to encounter some line than in New Jersey, although roughly two-thirds of voters in Virginia encountered no line. We do see that voters in precincts with DREs were more likely to wait in a line of any length to vote compared to precincts with optical scan voting or a mix of both technologies. However, voters in optical scan precincts were more likely than voters in DRE precincts (7.66% to 6.55%) to wait in a line that was 10 minutes or longer. Voters in precincts that had a mix of both technologies were least likely to wait in a line 10 minutes or longer.

4 Voter Confidence

One summary measure of the voting experience is whether the voter thinks that his or her vote was counted correctly. The standard metric for evaluating voter confidence has been to ask: "How confident are you that *your vote* in the General Election was counted as you intended?" In addition, some scholars have also begun to probe voter confidence in the count at higher levels of government; in this survey, we asked about confident in "your county or city" and in "your state as a whole." The purpose of asking all three questions is that one taps into a voter's confidence their the votes in their precinct will be counted, and the other two tap into confidence in the location where the votes are aggregated (in their city or county, where elections are administered in the United States) and were the final results are certified (at the state level).

Table 3 presents the percentages of respondents stating they were "very confident" in each state. The results are broadly consistent with other surveys of experience with government services, in which respondents generally report high ratings for their personal experience and lower ratings when asked about the experience of other people, or the system in general. In the November 2008 general election, 72% of New Jersey voters and 74% of Virginia voters said they were "very confident" their votes were counted as cast. The results for 2009 are very similar to those in 2008, with Virginia voters becoming slightly more confident and New Jersey voters slightly less confident. This might just be due to random variability, though the direction of the movements is consistent with the pattern that voters for winning candidates tend to express greater confidence than people who vote for the losers.

The New Jersey gubernatorial race was much closer than Virginia, which may explain some of the shift across the past year. Furthermore, when we look at how the confidence of partisans shifted between 2008 and 2009, the pattern is consistent with the "winners are more confident" theme. The next table reports the percentage of respondents saying they were "very confident" their own vote was counted as cast, by state and by party, across 2008 and 2009.

	Democrats			Republicans			Independents		
	2008	2009	Diff.	2008	2009	Diff	2008	2009	Diff
New Jersey	78%	62%	-16%	70%	76%	+6%	69%	66%	-3%
Virginia	81%	66%	-15%	71%	81%	+10%	68%	76%	+8%

Table 3: Change in Confidence, 2008 to 2009

In Table 4, when we consider confidence across various levels of government, we see that there is a clear decline in confidence as we move from the precinct to county to state levels. Over thirty percent of respondents were less confident in the overall state vote count than in how their own vote was counted. In Virginia, which has a non-partisan Board of Elections, 29% of Democrats and 25% of Republicans were less confident in the overall state vote count. In New Jersey, elections are run by an elections division that is located in the Secretary of State's office; the Secretary of State was associated with the unpopular Democratic governor. In New Jersey, 29% of Democrats and 39% of Republicans were less confident in the statewide count. In both states, roughly 35% of Independents were less confident in the statewide count.

	New Jersey	Virginia
Your Vote	68%	75%
Your City/County	54%	63%
Your State	41%	51%

Table 4: Voter Confidence Across Levels of Government

5 Voter Confidence and Technology

We also examined voter confidence across the various voting technologies used. Here, we see first that voter confidence varies across modes of voting. Absentee voters have the lowest level of personal confidence and Election Day voters have the highest levels of confidence. In Virginia, the personal confidence gap between Election Day and absentee voters is approximately 8 percentage points and in New Jersey, it is 14 percentage points. In New Jersey, the gap remains, but becomes smaller as we move to county-level and state-level confidence. In Virginia, the gap actually reverses at the state level, with absentee voters more confident than precinct voters. This reversal in Virginia largely occurs because precinct voters have more of a decline in confidence between personal and state confidence levels; the decline is much less for absentee voters.

In Table 5, we also see differences across the voting technologies used. In Virginia, some voters vote on DREs and some vote on optical scan. Most counties use only one technology or the other, but a small number of counties—including one of the most populous counties in the state, use a mix of optical scan and DREs in the precincts in the county. In Virginia, we see that DRE and optical scan voters have similar levels of confidence at all three levels and that individuals in counties with mixed technology are slightly less likely to be confident.

		New Jersey			Virginia		
		Not/Not Too Con-fident	Some-what Con-fident	Very Con-fident	Not/Not Too Con-fident	Some-what Con-fident	Very Con-fident
Mode of Voting	Election Day	4.17%	25.91%	69.92%	3.51%	20.02%	76.47%
	Early	20.00%	20.00%	60.00%	2.94%	23.53%	73.53%
	Absentee	10.13%	34.18%	55.70%	8.57%	22.86%	68.57%
Congruence: Technology Used and Wanted	Incongruence	11.01%	33.03%	55.96%	3.01%	26.42%	70.57%
	Congruence	3.94%	25.79%	70.27%	3.92%	17.84%	78.24%
Preferred Voting Method	Hand Count Paper	6.90%	37.93%	55.17%	2.33%	34.88%	62.79%
	Opscan	5.00%	41.67%	53.33%	6.14%	22.81%	71.05%
	DRE	3.85%	24.67%	71.48%	2.55%	16.41%	81.05%
Precinct Voting Technology	DRE	4.62%	26.61%	68.78%	3.99%	19.65%	76.36%
	Opscan				3.49%	17.44%	79.07%
	Mixed				3.18%	27.39%	69.43%

Table 5: Voter Confidence by Various Technology Factors

We also asked voters about their preferred method of voting. DREs were the top choice in both states, with 90% of New Jersey residents and 74% of Virginia residents making this choice. Optical scan was the choice of 6.7% in New Jersey and 21.2% in Virginia; hand counted paper ballots are the choice of 3.1% in New Jersey and 4.7% in Virginia. Some voters have congruence between their voting preference and the technology on which they vote; voters who want to vote on a DRE and vote in a precinct in New Jersey have such congruence, but voters who want to vote on a paper ballot that is counted via optical scan can only have such congruence if they vote absentee. A lack of such congruence could affect voter confidence, given that the voter would rather use a different technology.

When we examine confidence by preferred voting technology, we see that DRE voters are most confident that their vote will be counted accurately in both states. In Virginia, there is a monotonic decline in confidence from DREs (81% very confident) to optical scan (71%) to hand counted paper ballots (62.8% very confident). In New Jersey, the decline is roughly 15 percentage points from DREs to either optical scan or hand counted paper ballots. When we examine the issue of congruence, we see that voters who are congruent are more confident in both states, with the gap much larger in New Jersey than in Virginia. This is likely the result of it being difficult to vote using an alternate method in New Jersey, where absentee voting policies are not very liberal.

6 Voter Privacy and Problems at the Polls

The voting process is one that, since the turn of the 20th century, has been a private process with secret ballots. There is a normative idea that voting will be private, with ballots being secret. There is also an expectation that the voting experience will be problem-free and that voting technologies will work correctly. However, we have increasingly read of voters complaining that the in-person voting process is not private, either because voting booths are too small and exposed to wandering eyes, or because voters often have to hand a ballot to a poll worker to have it cast.[4]

In order to identify problems with the voting process and with privacy, we asked voters in both states the following question: "Do you agree or disagree that you were able to vote in private?" Overall, 91% of voters in New Jersey and 81% of voters in Virginia "strongly agreed" with this statement. It is not obvious why Virginia voters expressed less satisfaction with their voting privacy. The difference is not due to the presence of optical scanners in Virginia, since the percentages are virtually identical for users of DREs (80.6%) and optical scanners (81.4%). These differences persist across racial groups and types of communities. The robustness of the difference across the two states, regardless of controls for community and demographic factors, suggests that the explanation lies in the details of how precincts are configured in the two states.

We also asked voters, "Have you ever had a problem when you tried to vote that kept you from voting?" In Table 6, we see that, in New Jersey, 4.6% of voters said that they had had a problem that had prevented them from voting before and 3.6% of Virginians gave the same answer.[5] As we see in the table below, having a past problem voting or having concerns about voter privacy both affect voter confidence in a very negative manner. In New Jersey, privacy concerns lowered confidence by 19 percentage points; in Virginia, those with privacy concerns were 9.5 percentage points less confident than those who had no such concerns. Individuals who had encountered previous problems that kept them from voting were 25 and 20 percentage points less likely to be very confident in New Jersey and Virginia, respectively.

[4] For instance, see "New N.Y. Voting System Raises Privacy Concerns," pressconnects.com, http://www.pressconnects.com/article/20091130/NEWS01/911300341/New+N.Y.+voting+system+raises+privacy+concerns

[5] Voting machine problems were rather rare in this election, occurring in less than 1% of cases in either state.

	New Jersey			Virginia		
	Not/Not too Confident	Somewhat Confident	Very Confident	Not/Not too Confident	Somewhat Confident	Very Con-fident
Felt Privacy	4.02%	25.03%	70.95%	3.26%	19.59%	77.15%
Felt Lack of Privacy	11.63%	37.21%	51.16%	5.19%	27.27%	67.53%
No Past Problems	4.02%	26.03%	69.95%	3.40%	19.80%	76.80%
Past Problem Voting	20.00%	35.56%	44.44%	13.51%	29.73%	56.76%

Table 6: Confidence and Privacy

7 Voting Technologies and Voting Fraud

The role of computers in casting and counting votes has been a controversial issue since at least 2002 (AH04, AH08; HNH08; St06, St09]. The controversy over electronic voting centers, in part, over a debate as to whether paper ballots or electronic ballots are easier to count, easier to use for voting, and easier to steal. We asked these questions in New Jersey and Virginia with great interest because both states have substantial DRE usage. DREs are the sole technology used for in-precinct voting in New Jersey and approximately 75% of Virginia voters use DREs in the precincts.

	New Jersey			Virginia, DRE users			Virginia, OpScan users		
	OpScan	DRE	Paper	OpScan	DRE	Paper	OpScan	DRE	Paper
Easy to steal votes	59%	24%	80%	53%	23%	79%	30%	28%	75%
Easy for disabled	51%	70%	53%	54%	74%	56%	69%	63%	66%
Easy for non-disabled	69%	86%	69%	74%	89%	74%	84%	83%	84%
Easy to count	42%	77%	24%	51%	78%	28%	67%	68%	35%

Table 7: Concern About Voting Technology, by Voting Technology Used

We asked respondents their opinions of the three major voting technologies: (1) "paper ballots that are scanned and counted by a computer," (2) "electronic voting machines, that is, voting machines with a touch screen, like an ATM machine," and (3) "paper ballots that are counted by hand." For each of these technologies, we asked respondents to agree or disagree with the following statements about each technology:

1. It is easy for dishonest people to steal votes;
2. It is easy for people *with* disabilities to vote on;
3. It is easy for people *without* disabilities to vote on; and
4. It is easy for election officials to count votes accurately.

Responses to these questions are summarized in the previous table. The numbers in the cells are the percentage of respondents saying they *agree* with the statements. (Individuals saying they "don't know" are included in the denominator.)

Compare, first, the New Jersey respondents, all of whom used DREs if they voted in-precinct, with the Virginia respondents in DRE jurisdictions.[6] The attitudes toward the three technologies are strikingly similar. Virginians may be a little more favorably inclined toward all three technologies, but only slightly. For DRE users in both states, the superior technology is clearly DREs, followed by optical scanners and then hand-counted paper.

	New Jersey	Virginia	
Type of In-Precinct Equipment	DRE	DRE	Optical Scan
Paper ballot	3.0%	4.1%	4.4%
Optical Scan	6.3%	13.6%	40.0%
DRE	82.2%	76.7%	48.0%
Don't know	4.3%	2.9%	5.4%
Other	4.2%	2.8%	2.2%

Table 8: Preferred Voting Technology, by Voting Technology Used

When we compare the Virginia respondents who live in counties/cities that use DREs for in-precinct voting with those who live in municipalities that use optical scanners, we see that optical scan users have a better opinion of optical scanning than the DRE users, but except for the "vote stealing" item, the differences are surprisingly small. The same can be said for opinions about hand-counted paper ballots, as well. Similarly, optical scan users have a lower opinion of DREs than the DRE users, but the differences are surprisingly small, especially given the controversy over DRE machines. These findings lead us to conclude that voters are largely supportive of what they are currently voting on, with little nostalgic pining for the lowest-tech solution, hand-counted paper ballots.
We also asked the respondents "Which kind of voting machine or method would you most prefer to use?" Table 8 gives the responses to this question, broken down by state and by type of equipment use in Virginia. Again, users of DREs are happy to be using them, with New Jersey DRE users a bit more pleased with this technology than Virginians. In Virginia, the optical scan users are surprisingly split in their preference for the two major forms of voting.

Further analysis can be performed on these responses. The well-known divisions over machine choice show up in the data. For instance, liberals and highly educated respondents are more likely to oppose DREs. African Americans, interestingly enough, are more supportive of DREs in both states than are Whites.

[6] In New Jersey, 91% of voters in our sample report voting in a precinct on Election Day. In Virginia, the percentage was 93%.

8 Conclusion

Only quite recently have scholars begun to collect and analyze individual-level data on the voting experience in the United States. The availability of detailed individual data on a voter's experience, coupled with knowledge of what voting technologies are being used by these same voters when they cast their ballots, constitutes a rich new area for research and will no doubt generate new ideas for future improvement of election administration in the United States. We clearly see that voters are sensitive to the voting experience that they have and their attitudes about the electoral process are shaped in part by the experience that they have voting.

One of the most interesting results in our analysis concerns the confidence that voters state they have that their ballot is being counted as they intended. Consistent with earlier studies of voter confidence, we find that those who cast their ballot in person on Election Day express the most confidence that their ballot is being counted as they intended; those who vote before Election Day, especially those who vote by mail, consistently report lower levels of confidence that their ballots are counted as intended. Exactly why these differences exist in our analysis and in previous studies is a question that requires additional research, since increasing numbers of voters are choosing to cast their ballots before Election Day.

We also found that when voters were asked which voting technology they would prefer to use, we found that those who currently use DRE machines to vote would like to continue using them. Interestingly, we found that optical scan voters in Virginia were deeply divided about whether they would like to continue the use of optical scan voting technology, which indicates another area for future research.

The methodology used in this study—of surveying voters about their voting experience immediately after the election—is one that can be replicated in other countries and in all electoral environments. For instance, in the 2010 parliamentary elections in the United Kingdom, there were many reports of electoral problems, such as understaffed polling places, polls that ran out of ballots, and long lines.[7] A survey of voter attitudes can determine how such problems affect voter confidence and also identify the breadth of the problem nationwide, without having to rely solely on the media to know what occurred. For public managers of elections and for political principals, having these data can improve public management of election without having to rely solely on hearsay and media reports that are not validated with more systematic data.

[7] http://www.timesonline.co.uk/tol/news/politics/article7118998.ece

Bibliography

[Al09] Alvarez, R. M. 2009. Measuring Election Performance. Caltech/MIT Voting Technology Project Working Paper 94, http://vote.caltech.edu/drupal/node/325.

[AH08] Alvarez, R. M., & Hall, T. E. 2008. *Electronic elections: The perils and promise of digital democracy.* Princeton, NJ: Princeton University Press.

[AAB09] Alvarez, R. M., Ansolabehere, S., Berinsky, A., Lenz, G., Stewart III, C., and Hall, T. E. 2009. *2008 Survey of the performance of American elections.* Boston/Pasadena: Caltech/MIT Voting Technology Project.

[AHL08] Alvarez, R. M., Hall, T. E., and Llewellyn, M. 2008. Are Americans confident their ballots are counted? *Journal of Politics* 70 (3):754–766.

[AHL09] Alvarez, R. M., Hall, T. E., and Llewellyn, M. 2009. *The winner's effect: Voter confidence before and after the 2006 elections. Working Paper.* Pasadena, CA, http://vote.caltech.edu.

[AS07] Atkeson, L. R., and Saunders, K. L. 2007. Voter confidence: A local matter? *PS: Political Science & Politics* (40), 655-660.

[Be04] Bensel, R. 2004. *The American ballot box in the mid-nineteenth century.* New York: LOCATION: Cambridge University Press.

[BHC05] Bullock III, C. S., Hood III, M., and Clarke, R. 2005. Punch cards, Jim Crow, and Al Gore: Explaining voter trust in the electoral system in Georgia, 2000. *State Politics & Policy Quarterly* 5 (3):283-294.

[VTP01] Caltech/MIT Voting Technology Project. 2001. Voting: What is, what could be. http://vote.caltech.edu/drupal/node/10.

[CMM08] Claassen, R. L., Magleby, D. B., Monson, J. Q., and Patterson, K. D. 2008. At your service: voter evaluations of poll worker performance. *American Politics Research*, 36: 612-634.

[GHD09] Gerber, A., Huber, G., Doherty, D., & Dowling, C. 2009. Is there a secret ballot? Ballot secrecy perceptions and their implications for voting behavior. Paper presented at the annual meeting of the *American Political Science Association, .* Toronto, Canada, September 3-9, 2009.

[Ha09] Hall, T. E. 2009. *Voter attitudes toward poll workers in the 2008 election.* Pasadena, CA: Caltech/MIT Voting Technology Working Paper 77.

[HMP09] Hall, T. E., Monson, Q., and Patterson, K. 2009. The human dimension of elections: How poll workers shape public confidence in elections. *Political Research Quarterly* 62 (3):507-522.

[HNH08] Herrnson, P. S., Niemi, R. G., Hanmer, M. j., Bederson, B. B., Conrad, F. C., and Traugott, M. W. 2008. *Voting technology: The not-so-simple act of casting a ballot.* Washington, D.C.: Brookings Institution Press.

[KMN10] Karpowitz, C. F., Monson, J. Q., Nielson, L., Patterson, K. D., and Snell, S. A. 2010. *Political norms and the private act of voting. Working Paper.* Provo, UT: Brigham Young University.

[Ke00] Keyssar, A. 2000. *The right to vote.* New York: Basic.

[St09] Stewart III, C. 2009. Election technology and the voting experience in 2008. Paper presented at the annual meeting of the *Midwest Political Science Association,* Chicago, IL,: April 2-5, 2009.

[St06] Stewart III, C. 2006. Residual vote in the 2004 election. *Election Law Journal* 5 (2):158-169.

The Use of E-Voting in the Austrian Federation of Students Elections 2009

Robert Krimmer[1], Andreas Ehringfeld[2], Markus Traxl[3]
[1]E-Voting.CC gGmbH
Competence Center for Electronic Voting and Participation
1190 Vienna, Austria
r.krimmer@e-voting.cc

[2]Vienna University of Technology
Industrial Software (INSO)
1040 Vienna, Austria
andreas.ehringfeld@inso.tuwien.ac.at

[3]Institut für Verwaltungsmanagement
6020 Innsbruck, Austria
markus.traxl@verwaltungsmanagement.at

Abstract: The use of e-voting for the elections to the Austrian Federation of students (Hochschülerinnen und Hochschülerschaftswahlen) was one of the most sophisticated Austrian e-government projects in 2009. The task was to complement the paper based voting with an electronic voting channel in order to create new opportunities to vote. Together with the implementation of e-voting the legal basis of the federation of students was adapted to include an electronic election administration. The discussion around e-voting was rather controversial with clear pro and contra positions.

This first of a kind implementation of e-voting in Austria was technically successful. Almost 1% (2.161) of the eligible students cast their votes electronically between 18th and 22nd of May 2009. For identification and authentication, they used the citizen card (the Austrian model of a smart card with digital signature) and a suitable smartcard-reader device, which was handed out for free. The anonymity was performed by using a cryptographic protocol in the post-voting phase, similar to a paper based postal voting procedure. The e-voting servers were placed in two data centers of the Federal Computing Centre (Bundesrechenzentrum) to allow for fail-safe operation.

While the discussion around e-voting was rather controversial with clear pro and con positions, and marked a first nation-wide discussion around remote voting in general. For future uses of e-voting in Austria the penetration of identification and authentication means has to be raised as well as a more positive atmosphere amongst the stakeholders has to be reached.

1 Background

The first legally binding election offering a voting channel through the Internet in Europe took place at the University of Osnabrück (Germany) on February 2nd and 3rd of 2000 [FoIn00]. This served as the initial starting point for concrete thoughts around the use of electronic means in the elections to the Austrian federation of students. In May of that year the chairman of the federation of students took this as a reason to request the introduction of remote voting (either postal or Internet voting) to its elections in a public consultation process on the Hochschülerinnen- und Hochschülerschaftsgesetz (law on the federation of students) [Fais00]. Following this request a project group was installed consisting of members of the Federal Ministry of Science and the federation of students. This group decided to foster the development around electronic voting by piloting it at the Vienna University of Economics and Business Administration (WU). In the following months the legal grounds were laid for a first use in the federation of students elections (Hochschülerinnen- und Hochschülerschaftswahlen) taking place in spring 2001.

However in March of 2001 the project was stopped due to a continuous delay in the distribution of smart cards bearing a digital signature to the students of the WU [WUFl01].

Two years later the research group E-Voting.at at the Institute of Information Processing and Management at WU developed an E-Voting prototype for a shadow election in parallel to the paper-based federation of students elections in May of 2003 [PKKU03]. 978 students participated in this test where they cast an additional electronic to the paper vote. For the 2004 election to the Federal President this setup was repeated and a shadow election was conducted where all 20.000 students at WU could participate [PKKU04].
In the same year the then Federal Minister for Interior, Ernst Strasser, started an inter-ministerial working group to evaluate the constitutional, technical and international questions around a potential introduction of e-voting in Austria. This group recommended to first making experiences in elections to self-governing bodies like the chamber of commerce or the federation of students. Furthermore it came to the conclusion, in order to introduce e-voting on federal level it would need to be included in the constitution [AG04]. In 2007 a research assignment to the Federal Ministry of Interior was agreed in the coalition paper of the XIII. Government to investigate e-voting.

On May 11th 2007 the Federal Minister of Science Johannes Hahn announced publicly at a speech at University of Linz to offer e-voting for the first in the 2009 elections to the federation of students [Hahn07]. This was the basis for the first legally binding e-voting project in Austria.

2 The Project

The first step in this project was a feasibility study conducted in summer of 2007 [Krim07]. The main task was to integrate e-voting without compromising the existing paper-based voting in the polling station. To do so, an additional voting channel via the Internet was to be offered, from Monday 8:00 through Friday 18:00 in the week before the paper-based election days. During these days, all students of Austrian universities should have the possibility to participate in an Internet election without pre-registration. For identification purposes the Austrian citizen card (a smart card bearing a digital signature) in accordance with section 2 nr 10 of the Austrian E-Government law 2004 was to be used. After the end of the Internet-based vote casting, the votes were to be stored in an encrypted way until the general counting of votes at the end of the last voting day. Students, who had voted through the Internet, would be marked "voted" in the voter register and thereby guaranteeing the one-man-one-vote principle.
The next step was then to adapt the legal framework.

3 Legal Basis

The Federation of Students law 1998 (HSG) and the corresponding decree Federation of Students Election Regulations 2005 (HSWO) are the two legal texts forming the grounds for this project.
In Austrian self-governing bodies are regulated by national law passed by the parliament. In the course of the initial discussion around e-voting the national parliament passed an amendment to the Federation of students law in 2001 [HSG01]. It followed the principal of technology neutrality and only regulated certain corner stones. In section 34 paragraph 4 HSG 1998 the use of electronic signatures for identification purposes in accordance with the Austrian signature law, as well as the data protection law 2000 (DSG) were regulated. This led to the fact that for the e-voting system had to be approved by the Austrian data protection commission as it handles sensible data by interpretation of section 18 paragraph. 2 DSG. Furthermore the voting system has to provide technical means for the control of the electoral process to the election commissions.
The law also enabled the minister of science to introduce e-voting by the way of a decree, which included more detailed regulations for the e-voting system, like

- A definition of terms
- Change of time periods and mile stones for the electoral processes of the federation of students election
- Introduction of an additional voting channel
- Introduction of an election administration system

4 Diffusion of Smart Cards

A major challenge in the project was to distribute the Austrian citizen card amongst the students, as penetration with this technology was limited at the start of the project. For this the Austrian chancellery, the Federal Ministries for Finance and Science initiated the project studi.gv.at to foster the adoption of this new technology in fall of 2008. The project took place in parallel to the e-voting project due to synergies and both projects benefitting from each other. The main focus was to raise the public awareness amongst students for the citizen card itself as well as to promote services accessible with it.

The Austrian citizen card is an integral part of the social security card which every member of the Austrian social security system possesses[1]. To activate one's citizen card, a 10 minute procedure has to be done where a qualified person checks the activator's identity and then he/she can freely enter two PIN codes.

To raise the number of activations several activities were started

- The website studi.gv.at: this website provided information on the digital signature, the smart card itself as well as how students can make use of it. While in fall semester the focus was on general applications, the summer semester made a complete turn towards electronic voting as an application for the smart card.
- Distribution of free-of-charge card readers: Every student, who activated his/ her citizen card, got a card reader for free.
- Posters and flyers promoted the project.
- Tutors: As the activation required a qualified person, 22 tutors coming from different universities around the country who would then activate as many students as possible using a laptop with 3G data cards and explain the new technology to the potential users.
- As the project moved on, the tutors were trained to train other students for this activation procedure so that a snow-ball-effect could take place.

In general the project studi.gv.at was very successful as the number of citizen card users on paper reached 14.000. While in the beginning the numbers were rather low, the closer it got to the e-voting taking place in May 2009, the more students activated their smart cards. The project could be divided into four phases:

- Initial phase: October to December 2008
- Pre voting phase: January to April 2009
- Voting phase: May 2009
- Post voting phase: June 2009

[1] The citizen card basically is a functionality available not only to the social security card but also Austrian bank cards, credit cards etc.

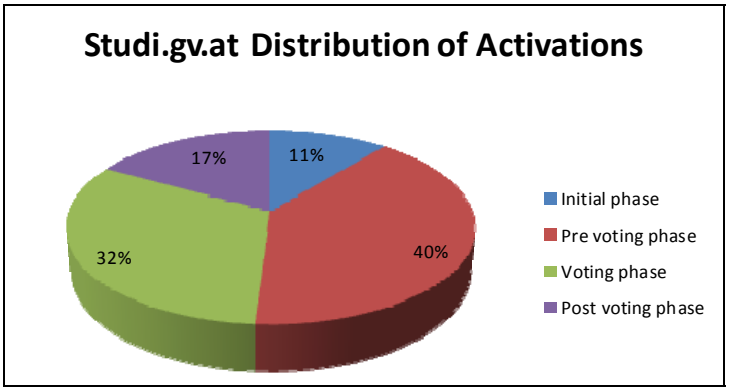


Figure 1: Distribution of Citizen Card Activations

4 The E-voting Process

The e-voting process from the point of the voter - amending it with certain steps happening in the e-voting application – took place as follows:

1. First the website https://www.oeh-wahl.gv.at was opened and then the voter chose the field "To the electronic vote"
2. Then the students selected the university at which he/she wanted to vote electronically. In case one wanted to vote for more than one university this step had to be repeated each time.
3. After the selection of the university the voter got concrete descriptions how to use his/her citizen card
    a. First the card reader had to be connected to the computer and the citizen card inserted
    b. Then the voter could either use a locally installed or a web-browser-based solution of the so-called citizen card environment, which basically is a driver set for web applications to access the smart card.
    c. Then the voter had to input a four-digit PIN-code which released his/her identity to the voting application
    d. This identification procedure was concluded with the authentication using the digital signature on the smart card which was activated by entering a six-digit PIN-code.

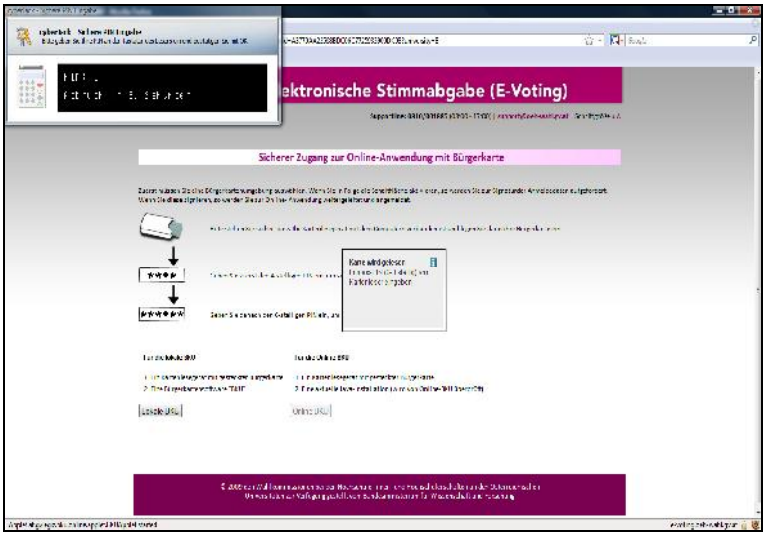


Figure 2: E-voting screenshot with PIN-code

4. After successful identification and authentication a ballot sheet was displayed for every race the voter was eligible to vote in. Normally an average students would cast two ballots
    a. The first ballot sheet was for the university board of the federation of students. Here one group could be elected.
    b. The second and more ballot sheets were for the study board representation. Here up to five student representatives could be elected.
5. Invalid votes could be cast by either not selecting any choice or by selecting too many.
6. After all ballots were cast an overview with all choices was displayed to the voter and had to be confirmed. This should prevent junk votes.
7. The confirmation took place with an affidavit where the voter confirmed to have cast the ballot in person and not have been influenced by a third person. This had to be signed digitally again with his/her six digit PIN-code.
8. The voting system showed after the successful vote a confirmation code. This code could be used after the end of the election to check whether one's vote was counted.

In the following figure we tried to amend this process with the cryptographic steps taking place similar to the process when filling out a postal vote.

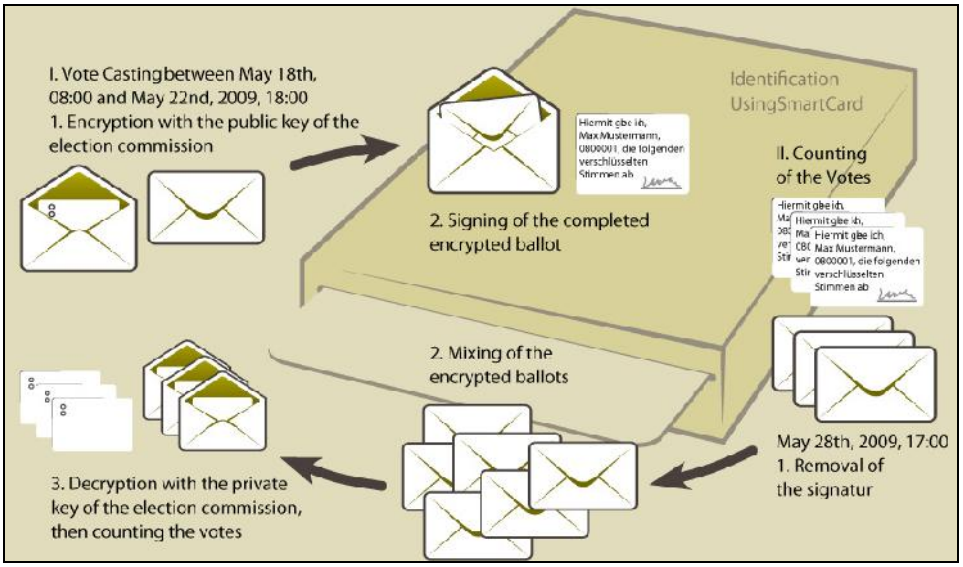


Figure 2: Overview of the E-voting Process

5 Pre Voting Phase

The project can be divided into three phases – (i) the pre voting, (ii) the voting, and (iii) the post voting phase. While the voting phase was the most intense period, the preparatory steps were manifold. A first step was the certification process.

5.1 Certification

The components of the e-voting system, which were used for vote casting and verification of the voters' identity, had to be certified 60 days before the first day of use by the independent certification body A-Sit established by the Austrian signature law[2]. The standard against which the e-voting system is checked against was the Council of Europe recommendation on legal, operational and technical standards for electronic voting [CoE04].

[2] The legal basis is laid down in section 64 paragraph 3 HSWO 2005 and section 34 paragraph 6 HSG 1998.

The certification lasted from December 1 2008 till March 25 2009 and was conducted using the source code as well as technical documents written by the e-voting provider. A-Sit checked whether the security architecture of the software was able to fulfill the requirements in the law. Furthermore the source code was used to verify if the described architectural protection methods were also implemented correctly. On March 27 2009 A-Sit published the certification [ASit09].

5.2 Usability Test

On March 18 2009 two universities[3] conducted a usability test. Aim was to verify the actual ease of use of the e-voting system and to collect feedback from the students. These comments were reviewed critically and implemented in the final version of the software.

5.3 Vote Eligibility Check

The vote eligibility check was offered from 23rd to 30th of April 2009. This was the first possibility to use the citizen card within this project. Here a single voter could check his/her own eligibility to vote. Around 370 persons made use of this opportunity. It was noted that a number of people had problems remembering their PIN-codes for the citizen card. During the whole time of the eligibility check a support hotline was offered.

In case a voter found an error with his/her personal voting rights, he/she had the possibility to appeal against it with the election commission at the respective university. On the basis of these appeals missing voting rights were corrected after decision by the election commissions.

5.4 Review of Certification Report by Members of the Election Commissions

The minister has to provide members of the election commissions following section 64 paragraph 3 and 7 HSWO 2005 with the possibility to review the certification report and the source code of the e-voting system software.
This review took place on 8th of May 2009. The participants had to sign up for this occasion. Based on the regulation only members of the elections commissions were allowed to participate, which count for 250 persons.
The review meeting was designed to accommodate all of them, however only 28 took part in the event. At the beginning the agenda was discussed with the participants. It was arranged in sessions, where experts – including the developers of the system – presented the underlying principles. In parallel the certification report and the source code could be reviewed and questions asked to the experts.

[3] Vienna University of Economics and Business Administration and University of Leoben

5.5 Fail-safe Operation of the E-voting Servers

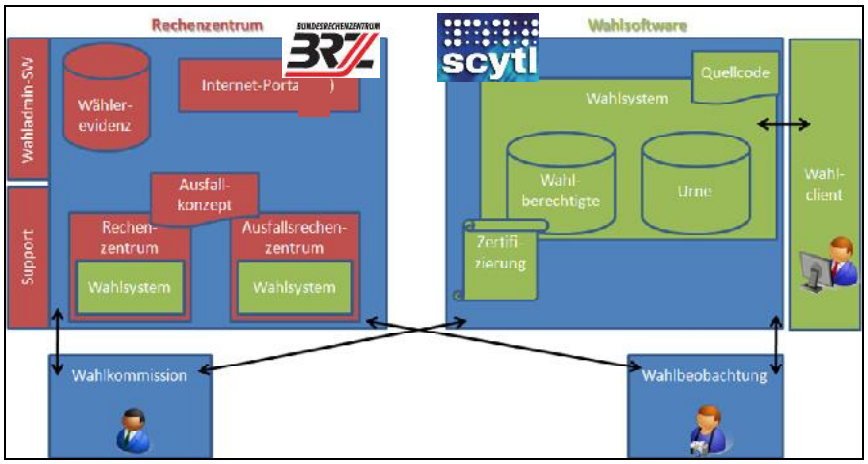


Figure 3: Overview Infrastructure

The servers were operated at two separate locations:

- Federal Computing Center (Bundesrechenzentrum GmbH)
- Parallel Computing Center

The two computing centers were about five kilometers apart from each other. Both locations met highest international standards regarding physical security, energy supply, fire protection, access control systems, recording systems (real time video surveillance, access logging).

The e-voting system was classified as highly critical system and was underlying special security mechanisms within the federal computing center (BRZ).
All components were put in a security rack in each computing center location. Access to the protected zone around the security rack in the server room was only possible for authorized personnel. Access of any kind was logged and controlled by the security control center.

Additionally both security racks were secured using steel cables and cable seals from the point of installation till the secure data destruction. Each single cable seal was registered using a unique number.

Figure 4: Sealed security rack

5.6 Ethical Convention on E-voting

In the field of e-voting the Council of Europe has developed with the 2004 recommendation on legal, operational and technical standards [CoE04] a very important instrument. Since then it has observed the developments in its member countries on this issue. In communication with the federal election commission of the federation of students elections, the Council of Europe recommended them to publish an ethical convention on e-voting based on the experiences in Estonia [TSBA07]. The commission developed an initial version and forwarded it to the commissions at the respective universities. For future elections it deems necessary to make a broad discussion process on this convention in a timely distance to the election days (on a political level and also in the public sphere).

6 The Voting Phase

230.479 students were eligible to vote at the 21 Austrian universities where the federation of students elections 2009 took place. A total 375 races had to be decided, consisting of 21 university body elections and 354 study body elections. 2,411 candidates campaigned for 1,633 mandates.

On Monday, 18th of May 2009 at accurately 8:00 the electronic voting was started. The system automatically opened the vote casting which was observed by several representatives of the media. Shortly afterwards the first legally binding vote was cast successfully.

The electronic voting ended technically successful on Friday, 22nd of May 2009 at 18:00. Until then 2,161 students participated in the elections.

During the electronic voting the servers and the number of participants at the 21 universities could be watched in a 24hrs accessible observation room at the federal computing center. There a screen was directly attached at the database server to allow for election observation.

On the first two days of the e-voting the Austrian Federal Ministry of European and International Affairs had organized an international seminar on voting from abroad. The participants watched the whole process and concluded that e-voting election observation must allow for an end-to-end observation of all process steps. An observation solely on election day allows only for limited assessment [VEVS09].

After the e-voting voting channel was closed, the voter directories at the universities were updated in accordance with which voting rights were used by participants in the e-voting. The paper based election took place from Tuesday, 26th to Thursday 28th of May 2009. Here for the first time an election administration system was offered to all election commissions at the 21 universities, including the approximately 50 sub-commissions.

7 Post Voting Phase

In the post voting phase the counting of the votes was started right after each polling station had closed. While the paper-based votes were counted right at the respective polling stations, the electronic votes got counted at the Federal Computing Center where representatives of the federal election commission of the federation of students elections were present, as well as from certification body A-Sit, and the operational team from the Federal Computing Center, after the last polling station had closed at 17.00. After detailed security and documentation procedures were completed it took only 1.5 hours in total to come up with the final e-voting results. A special challenge was the aggregation of the electronic and paper-based results, as some election commissions had problems to operate the election administration system which was used for this purpose. This was especially unfortunate as this led to a disappointment with the media for whom e-voting mainly is a tool for faster results calculation.

Three weeks after the election days all data – but the votes and protocols – were destroyed using physical and then thermal destruction.

8 Conclusions

In this Austrian premiere with a the first implementation of a remote electronic voting channel in a legally binding election it was shown successfully how a participation via the Internet is possible in a political decision making process. Hereby many experiences – common to pilot projects – were made. This includes especially the adaptation of paper election processes to the requirements of processing electronic votes as well as the intensive public discussion. Especially the public discourse had to be led and was very important especially to the topic of e-voting as well as to the discussion remote voting channels in Austria in general.

Bibliography

[AG04] Arbeitsgruppe ‚E-Voting' (2004): Abschlussbericht zur Vorlage an Dpr. Ernst Strasser, Bundesminister für Inneres, Wien, http://www.bmi.gv.at/wahlen/wahldownloads/E-Voting/Abschlussbericht_E-Voting_2004_11_29.pdf

[ASit09] A-Sit Certification, published at http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_hsg/index.php

[CoE04] Council of Europe: Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11, Council of Europe, Strasbourge 2004.

[Fais00] Faißt, Martin: Stellungnahme der Österreichischen Hochschülerschaft anlässlich der Änderung des Bundesgesetzes über die Vertretung der Studierenden an den Universitäten – Hochschülerschaftsgesetz 1998, May 15 2000.

[FoIn00] Forschungsgruppe Internetwahlen, Zweiter Zwischenbericht zum Projekt ‚Strategische Initiative: Wahlen im Internet' nach Abschluss der Wahlen zum Studierendenparlament der Universität Osnabrück am 2. Feb. 2000, Osnabrück, 2000.

[Hahn07] APA: Wissenschaftsminister Hahn will E-Voting bereits bei ÖH-Wahl 2009. Aussendung APA0431, May 11 2007, Vienna.

[HSG01] Hochschülerinnen- und Hochschülerschaftsgesetz 1998, passed on Feb. 1, 2001.

[Krim07] Krimmer, Robert: Machbarkeitsstudie – Durchführung der Hochschülerinnen- und Hochschülerschaftswahlen mittels elektr. Abstimmungsverfahren, Vienna, 2007.

[TSBA07] Trechsel, A., Schwerdt, G., Breuer, F., Alvarez, M.(2007): Internet Voting in the March 2007 Parliamentary Elections in Estonia, Florenz, http://www.vvk.ee/public/dok/Coe_and_NEC_Report_E-voting_2007.pdf

[PKKU03] Prosser, Alexander; Kofler, Robert; Krimmer, Robert; Unger, Martin-Karl (2003): Die erste Internet-Wahl Österreichs. Working Papers of the Institute for Information Processing and Management, Nr. 04/2003, http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01_574.pdf?ID=epub-wu-01_574

[PKKU04] Prosser, Alexander; Kofler, Robert; Krimmer, Robert; Unger, Martin Karl (2004): E-Voting Wahltest zur Bundespräsidentschaftswahl 2004, Working Papers of the Institute for Information Processing and Management, Nr. 01/2004, http://epub.wu-wien.ac.at/dyn/virlib/wp/mediate/epub-wu-01_714.pdf?ID=epub-wu-01_714

[VEVS09] Bundesministerium für europäische und internationale Angelegenheiten: E-voting seminar. http://www.bmeia.gv.at/botschaft/auslandsoesterreicher/ratgeber/wahlen/e-voting-workshop-2009.html

[WUFl01] Hochschülerinnen- und Hochschülerschaft an der Wirtschaftsuniversität Wien (2001): WU-Flash, Ausgabe 025, Newsletter May 5 2001, http://flash.oeh-wu.at/pipermail/wu-flash/2000-May/000037.html

Scantegrity Mock Election at Takoma Park

Alan T. Sherman (UMBC)[1], Richard Carback (UMBC),
David Chaum, Jeremy Clark (UWaterloo),
Aleksander Essex (UOttawa), Paul S. Herrnson (UMCP),
Travis Mayberry (UMBC), Stefan Popoveniuc (GWU),
Ronald L. Rivest (MIT), Emily Shen (MIT),
Bimal Sinha (UMBC), Poorvi Vora (GWU)

[1]Contact author: Cyber Defense Lab
University of Maryland, Baltimore County (UMBC)
Baltimore, MD 21250, USA
sherman@umbc.edu.

Abstract: We report on our experiences and lessons learned using Scantegrity II in a mock election held April 11, 2009, in Takoma Park, Maryland (USA). Ninety-five members of the community participated in our test of this voting system proposed for the November 2009 municipal election. Results helped improve the system for the November binding election.

1 Introduction

On April 11, 2009, ninety-five voters cast ballots on the Scantegrity II voting system during a mock election held at the Community Center in Takoma Park, Maryland, coinciding with Takoma Park's celebration of Arbor Day. The purpose of this exercise, which we call Mock1, was to demonstrate and tune Scantegrity's capability in preparation for the Takoma Park municipal election in November 2009 [Car10]. The November election was historic — the first time any end-to-end (E2E) cryptographic voting system with ballot privacy has been used in a binding governmental election. This paper, a short summary of which appears as [She09], describes our experiences using Scantegrity in Mock1 and presents and interprets data collected through questionnaires, unobtrusive observations, and independently-administered focus groups.

Scantegrity [Cha09] is a software-independent cryptographic audit system that overlays a traditional optical-scan voting process. Voters mark paper ballots with revealing ink, exposing a randomly chosen confirmation code in each marked oval, which the voter may choose to write down on a detachable ballot chit. After polls close, each voter has the option of checking her confirmation codes online, to verify that her vote has been recorded as intended. Furthermore, Scantegrity is universally verifiable: using special software of his or her choice, anyone can verify online that the tally was computed correctly from the official data (and during the actual election, two auditors even wrote their own software for this purpose and made it public).

There has been some debate within the voting systems' community about how easily cryptographic end-to-end systems could be understood, used, and administered, but there is little evidence from which to draw any conclusions.

Mock1 is part of a larger research project to measure how easy Scantegrity is for voters to use and poll workers to administer. The research also studies how well voters and poll workers accept this revolutionary system. Mock1 only tested the Scantegrity voting system and was required to mimic a binding election. We closely followed procedures that were later used in November's binding election. These requirements constrained research methodologies, but were needed to assess viability of Scantegrity in the binding election. We plan to carry out a second mock election, Mock2, and expert review, which will be a field test comparing Scantegrity with a commercial optical scan voting system.

Our hypothesis is: Voters and election officials will accept and have confidence in Scantegrity as a viable practical high-integrity voting system. They will find it reasonably easy to use and administer, compared with traditional optical scan voting. A statistically significant number of voters will verify their votes online, and a statistically significant number of them will detect errors, if present, to produce high assurance in the election outcome.

At Mock1 we measured Scantegrity's performance through surveys, observations, and focus groups. Eighty voters and all six Takoma Park poll workers filled out questionnaires about their experiences with Scantegrity, including questions about how easy the system was to use and administer and how well they understood and accepted the system. Two unobtrusive observers watched and timed fifty-three of the voters as they voted. A professional moderator led two focus groups: one for all six poll workers and one attended by four voters. After polls closed, twenty-nine of the voters (31%) verified their votes online, using a privacy-preserving receipt on which each voter copied confirmation codes exposed during the voting process for their ballot choices.

In the rest of this paper, we briefly review selected previous work, explain our election and research methods, present and discuss our results, state recommendations, and explain our conclusions. The Scantegrity website [Scan] lists additional details about Mock1, including questionnaires and the agreement with the City of Takoma Park.

2 Previous Work

There have been several usability studies on voting systems and vote-verification systems, but no major usability study has been conducted on any E2E voting system. The only previous usability studies on E2E systems have been the preliminary studies mentioned above and a few student projects at UMBC (on Punchscan), MIT (on ThreeBallot), and Univ. of Surrey, England (on Prêt à Voter). Scantegrity and its predecessor Punchscan [Punch] were exercised by running student elections, organizational elections, mock elections, the 2007 VoComp International Voting System Design Competition [Voc07], and surveys [Scan]. Scantegrity has been used at the following events: Mock Presidential Elections at MIT and George Washington

University (November 4, 2008, Cambridge, MA, and Washington, DC); Mock Board of Directors Election for the Ottawa Canadian Linux Users Group (April 1, 2008, Ottawa, Canada); and a survey at the Claim Democracy Conference (November, 2007, Washington, DC). Essex *et al.* [Ess07] document their use of Punchscan in the 2007 student elections at the University of Ottawa.

RIES [OSCE07, Hub05] was used twice in 2004 in the Netherlands in a government Internet election. This system is voter verifiable and universally verifiable, but allows voters to prove how they voted. Helios [Adi09] was used in March 2009 to elect the President of the Université catholique de Louvain using remote voting. This system neither protected against undue influence nor compromise of the voter's computer. Byrne *et al.* [Byr07] experimentally compared the usability of punch cards, lever machines, and paper ballots; they found that voters made fewer errors with paper ballots.

Using expert review, laboratory studies, and a field experiment with 1540 participants, Herrnson *et al.* [Her08, Bed03, Con09, Her06] found that voting system interface and ballot styles had an impact on voter satisfaction, the need for help, and voters' abilities to cast their ballots as intended. They also demonstrated that the most frequent error made by voters was voting for a candidate other than the one they intended to support, usually a candidate listed on the ballot immediately before or after the intended candidate. This type of error is more serious than the errors associated with the residual vote because, in addition to denying an intended candidate a vote, it gives a vote to a candidate's opponent. They found that results of this experiment varied by voter demographics and voting experience. They also found that design issues and voter backgrounds influenced not only the voters' evaluations of different voting systems, but also their voting accuracy. Laskowski [Las04] offers practical metrics for voting system usability, and draft voluntary guidelines [EAC07] address usability.

There is a large body of knowledge about the usability of both computer systems [Shn05] and security [Cra05], but none of this work addresses how well and easily voters and election officials will be able to use Scantegrity.

Alvarez *et al.* [Alv08] and Newkirk [New08] frame public opinion about voting technologies. Newkirk finds that public opinion about voting systems has remained remarkably stable between 2004 and 2008. Direct Recording Electronic (DRE) systems were the top-rated systems in terms of voter trust throughout most of this period, followed closely by precinct count optical scan (pcos) systems. Fewer voters trusted vote-by-mail, central count optical scan systems, and Internet voting. There were some variations by background characteristics, but the overall stability in levels of trust and the near parity of DRE and pcos systems are remarkable given questions raised about these systems by serious scholars, political activists, and conspiracy theorists on the blogosphere. Indeed, public confidence in election count accuracy was ranked only second to public trust in banks and financial institutions. More confidence was voiced for elections than medical providers (including hospitals and clinics), universities and schools, large corporations, and the government.

Given the impact of public opinion on the decisions of policymakers who purchase voting systems and oversee other matters related to the administration of elections, it is important to study public reactions to voting systems. The fact that no such study has been conducted on any E2E system to date is a significant shortcoming. The Mock1 test of Scantegrity is a first step in addressing this shortcoming.

3 Methods

We now describe the voting and research procedures used in Mock1. Our research protocols and questionnaires were approved by UMBC's Institutional Review Board, as required for experiments with human subjects. Polls were open from 10 AM to 2 PM

3.1 Voter Experience

Each voter first approached a welcome table located outside the polling room. After signing a consent form, the voter proceeded to an adjacent check-in table. There, a poll worker looked up the voter's name in a poll book and issued a voter authority card. The voter then entered the polling room and presented the voting authority card to poll workers at the ballot issue table, who issued a Scantegrity ballot secured to a locked clipboard with privacy sleeve (see Appendix B).

The voter proceeded to one of three voting areas, each with a cardboard privacy shield. Using a special pen with revealing ink, the voter marked her ballot choices by marking the selected ovals with the pen. The revealing ink exposed a two-character confirmation code in each marked oval. Optionally, while also using the special pen, the voter could write down these confirmation codes on a detachable ballot chit, treated with reactive ink. As required by Takoma Park for municipal elections, Instant Runoff Voting (IRV) [Pou08] was used, so each voter was asked to rank each candidate in order of preference.

Appendix A shows the Mock1 ballot, which featured four questions about trees. To avoid possible confusion, Takoma Park officials required that races on our Mock1 ballot not resemble those on official ballots. November's official ballot had two races (mayor and ward council member) per ward. The municipal election can also have ballot questions.

Instead of voting on the issued ballot, each voter had the option of performing a "print audit" to verify that the ballot had been correctly printed. To do so, the voter walked to a voter assistance table and followed instructions from a poll worker. The poll worker marked the ballot spoiled and exposed all confirmation codes. The voter was permitted to copy information from the ballot to take home. A poll worker then escorted the voter back to the ballot issue table to receive another ballot. Each voter was allowed to receive up to three such ballots. We used a similar procedure if the voter unintentionally spoiled a ballot (e.g., by marking the wrong choice).

After marking the ballot, the voter proceeded to the scanning table. A poll worker unlocked the ballot from the locked clipboard and scanned the ballot. Looking at a touch-screen display connected to the scanner, the voter confirmed that the ballot was scanned. Without showing the voter's ballot choices, the touch-screen display warned the voter if the scanner detected any over- or under-voted questions. At this point, the voter could either return to the voting area with the ballot or cast the ballot by pressing the cast button on the display. The poll worker then tore off the chit and gave it to the voter, and dropped the ballot into the ballot box. Throughout the scanning process, a privacy sleeve hid the ballot choices. The chit provided instructions on how the voter could optionally verify her vote online after polls closed.

3.2 Research Protocols

Any consenting adult who showed up was permitted to vote. At the request of Takoma Park, to encourage children to become involved in voting and new voting technology, assenting children twelve to seventeen years old were also permitted to vote, with parental consent. We advertised the event through e-mail, Web pages, local TV, and in the Takoma Park Newsletter [TPN09]. Despite the rain, 105 people signed consent forms.

Sitting in the polling room in the place reserved for official observers, two unobtrusive observers watched as many voters as possible, filling out voter observation sheets. Each observer recorded the time an observed voter spent from receiving a ballot to casting it. Each observer also noted how many times the voter spoiled a ballot, requested or received assistance from a poll worker, or appeared confused.

As each voter left the polling room, a researcher asked the voter if she would be willing to fill out a questionnaire. If yes, the researcher handed the voter a conventional clipboard with two two-sided questionnaires: a voter field test questionnaire and a demographics questionnaire. Form numbers linked the field test and demographics questionnaires filled out by the same voter.

As the voter returned the clipboard, the researcher asked the voter if she would be willing to return at 3 PM that day for a one-hour focus group. For each such willing voter, the researcher wrote down a telephone number and the demographics form number. The plan was to call eight of the willing voters, reflecting a diverse sample of voters as determined solely from the demographics form. However, given that only twelve of the 80 voters filling out questionnaires agreed to participate in a focus group, we invited all twelve willing voters, of whom four showed up.

We also conducted a separate one-hour focus group for all six poll workers as soon as possible after polls closed. Each poll worker also filled out a poll worker field test questionnaire and demographics form.

Voters could visit the online verification web site after polls closed. After providing consent and verifying their votes online, they were invited to fill out an online verification questionnaire and a short demographics form.

Aside from the consent form and list of telephone numbers on the focus group sign-up sheet, we did not collect any personal identifying information.

Originally, we had planned to link each voter's demographics questionnaire to her observation sheet and ballot (and thereby to her verification questionnaire). Ultimately, we decided not to do so, to avoid interfering with the election process, and to avoid creating the appearance of violating ballot privacy. Instead, we added a second short demographics questionnaire to the online verification experience.

For Mock1, Takoma Park poll workers and Scantegrity team members worked side-by-side to help the poll workers learn how to operate the system. By contrast, in the binding election in November, poll workers operated the system entirely by themselves.

4 Results

This section summarizes data collected from our research instruments, including the voter demographics questionnaire, observations sheets, voter field test questionnaires, online voter demographics and verification questionnaires, and the voter and poll worker focus groups.

4.1 Unobtrusive Observations

Figure 1 summarizes observations made by two unobtrusive observers watching fifty-three of the voters. The main difficulty was the length of time it took to vote, averaging about eight minutes from the time a voter received a ballot to the time the voter cast the ballot (not including time for check-in or instructions given before voter received a ballot). Much of the time was observed to be at the scanner table.

When voters asked for assistance and/or poll workers intervened, it was typically either because the voter did not know what to do after marking the ballot, or because the voter did not know what to do upon spoiling a ballot.

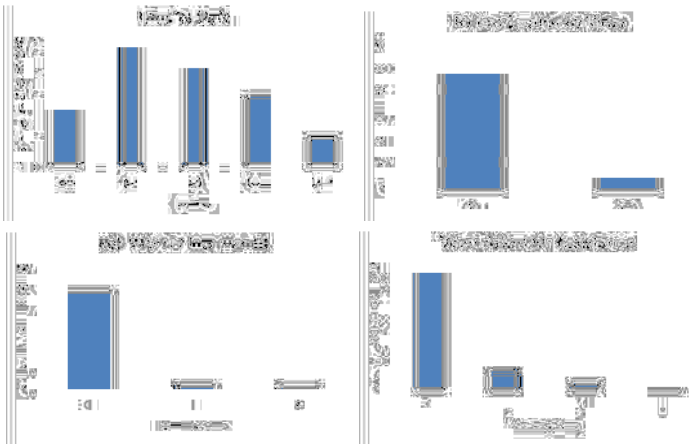


Figure 1: Summary of data from unobtrusive observations of 53 voters.

4.2 Voter Demographics

Figure 2 summarizes voter characteristics of the eighty voters who filled out paper demographics questionnaires. These voters were not representative of the Takoma Park voting population. They had high family incomes and were highly educated, frequent computer users, mostly fifty to sixty years old, motivated, and able to get to the mock election on their own.

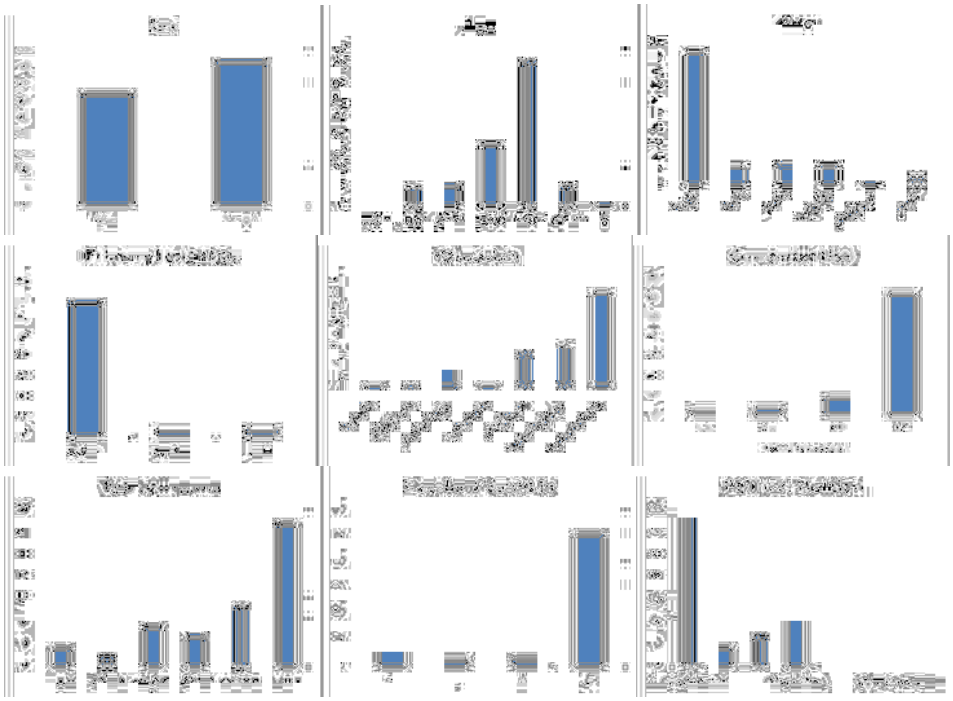


Figure 2: Summary and comparison of voter demographics from 80 responses to a paper questionnaire filled out by voters immediately after voting.

4.3 Voter Field Test Survey

Figures 3 through 6 summarize data collected from eighty field test questionnaires filled out by voters immediately after casting their ballots. We include all responses, even though it was apparent (from implausible answers to questions about ease of correcting errors and understanding of cryptographic details) that three respondents had likely reversed the seven-point Likert scale.

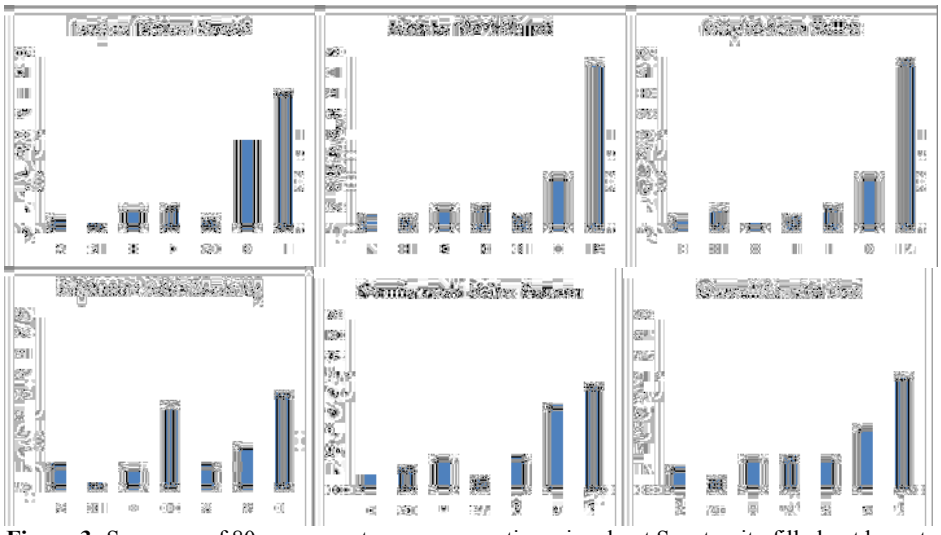


Figure 3: Summary of 80 responses to a paper questionnaire about Scantegrity filled out by voters immediately after voting.

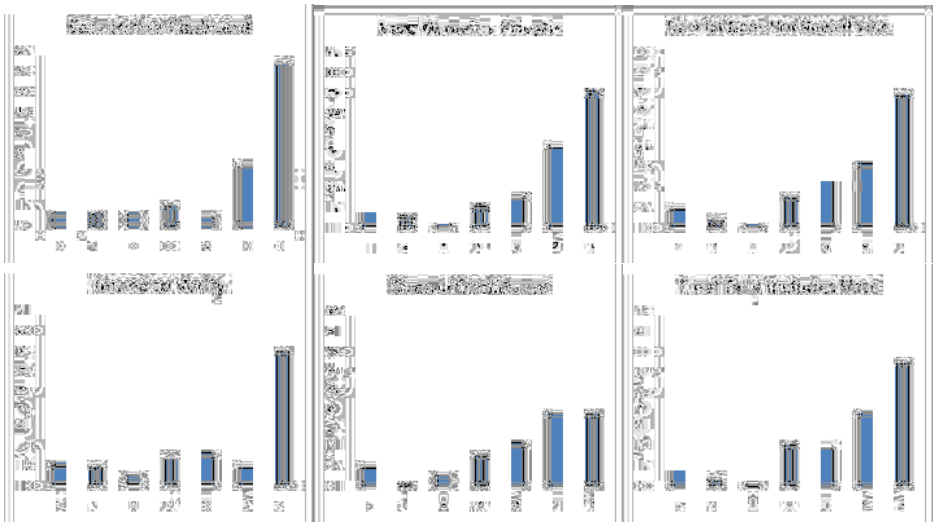


Figure 4: Summary of 80 responses to a paper questionnaire about Scantegrity filled out by voters immediately after voting.

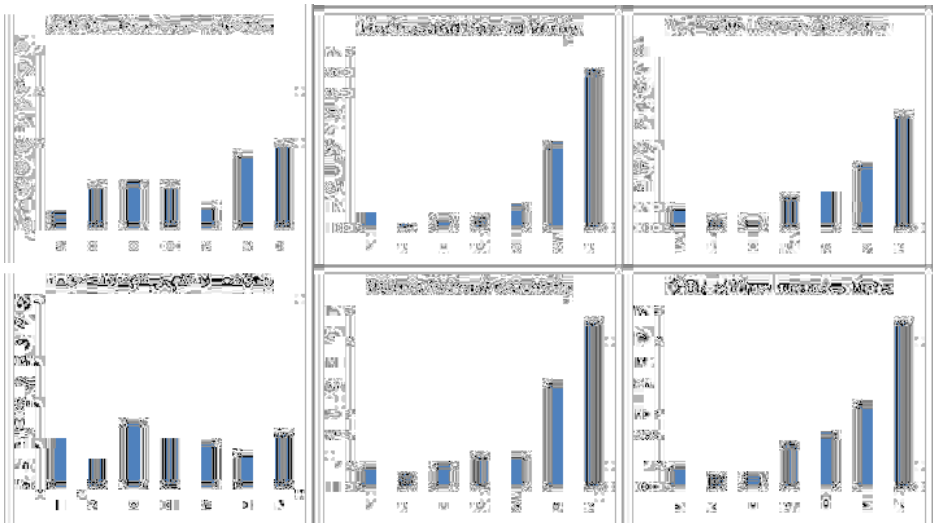


Figure 5: Summary of 80 responses to a paper questionnaire about Scantegrity filled out by voters immediately after voting

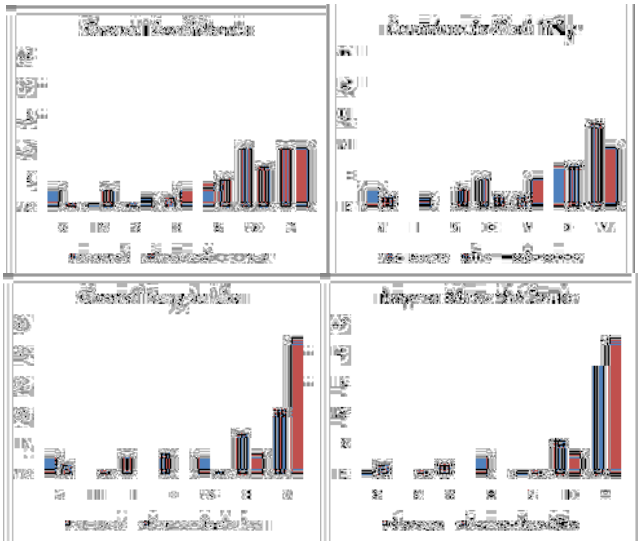


Figure 6: Summary of 31 responses to questions about Scantegrity and a comparison to answers from those same responders about traditional optical scan systems based on their recollection of their last experience with an optical scan system (1 = strongly disagree, 7 = strongly agree)

4.4 Online Voter Verification Survey

As of April 15, thirty-one voters verified their votes online. Seven of these voters completed the associated online questionnaire. Table 1 summarizes the responses from these seven voters.

Q		1	2	3	4	5	6	7
1	I was able to complete the verification process.	0	1	0	0	0	2	4
2	I verified that my votes were correctly recorded as cast.	1	1	0	0	0	2	3
3	The verification system was easy to use.	1	0	0	0	0	1	5
4	I feel comfortable using the verification system.	1	0	0	0	0	3	3
5	I am confident the official data includes my intended vote.	0	1	0	2	1	1	2
6	I am confident the final tally includes my intended vote.	0	1	0	3	0	1	2
7	I am confident my vote is and will remain private.	0	1	0	1	2	2	1
8	Online verification increased my confidence in the results.	1	2	1	1	1	0	1
9	I understand how the online verification system works.	0	3	1	0	0	1	2
10	I have confidence in the online verification system.	0	1	0	4	1	0	1
11	Overall, I have confidence in Scantegrity.	0	0	1	3	2	0	1

Table 1. Summary of all 7 responses from the online verification questionnaire (1 = strongly disagree, 7 = strongly agree).

4.5 Voter and Poll Worker Focus Groups

Four voters participated in the voter focus group. These came from the twelve voters who stated they might be available to participate, all of whom were invited. These four voters were not representative of the Takoma Park voting population: they were involved with municipal functions and some had helped bring voters to previous elections.

All six Takoma Park poll workers participated in the poll worker focus group. Each was experienced and had worked previous elections in Takoma Park. None are part of the Scantegrity Team. Because both groups expressed similar thoughts, we now summarize the main comments from both groups together, as reported by the moderator [Bau09]:

1. The process took too much time.
2. Providing instructions in one chunk at beginning was overwhelming.
3. The instructions were too complex, and there was too much explaining.
4. Although the voters in the focus group did not experience difficulties voting, some wondered if other voters in Takoma Park might experience difficulties writing down confirmation codes and verifying their votes online.
5. Vote casting at the scanning table took too much time.
6. Some poll workers disliked that a poll worker handled the ballot during scanning.
7. The scanner was finicky.
8. During scanning, the poll workers liked the feedback of seeing light on a flash drive blink, suggesting that the ballot was read.

9. The locked clipboard added time and complexity, but did not increase security.
10. Make the special pens available only in the voting area.
11. Poll workers felt that they should have been more in charge, especially of the flow of voters around the room.
12. Poll workers felt that the process could be sped up to make it viable for the binding election.

Finally, the moderator [Bau09] emphasized, "It is critical that all instructions are tested ahead of time on a range of people representative of the wider Takoma Park population to ensure they are clear and understandable" and that "[t]ranslations into other languages must also be tested."

5 Discussion

The main two issues were that the process was too slow (taking about eight minutes to vote on average) and many voters found the instructions somewhat complicated. Much of the delay was caused by the scanning process and lengthy instructions given to voters. Fortunately, these problems are solvable through process simplification and improvement, better scanners, and careful human-factors testing.

Although there has been tremendous simplification of Chaum's ideas from SureVote, through Punchscan to Scantegrity, the team had spent relatively little effort on testing and perfecting the human-factors details of the voting process, especially when carried out by typical voters. Some Mock1 voters were enthusiastic about the security features of Scantegrity, but most seemed not to care much about security, focusing primarily on the physical process of receiving a ballot, marking the ballot, and scanning the ballot. While such voter reactions are well known from the social science literature, it was nevertheless a dramatic learning experience to witness these reactions first-hand.

Although the Mock1 voters and participants in the voter survey group were not typical Takoma Park voters (many were self-selected as having an interest in the voting system to be used by the city, and some were just there to participate in the Arbor Day celebration), they provided useful feedback and expressed awareness of potential issues that might affect other voters. Factors affecting the slow voting process included lengthy instructions, redundant instructions, instructions for optional steps, use of the locked clipboard, writing down confirmation codes, tearing off the ballot chit, difficulty of correcting mistakes (for the few who unintentionally spoiled ballots), checking for over- and under-votes at the scanner touch screen, and a slow, finicky scanner.

Our scanner caused significant problems. Ballots had to be inserted in a particular orientation. If they went in at too much angle, a corner could be unread. Some voters seemed confused that the touch screen did not show how they voted, but only for each race whether the race was over- or under-voted. After the voter pressed "cast," feeding the scanned ballot into a privacy sleeve and dropping the ballot into a large ballot box was clumsy. Although these equipment, implementation, and process problems can be fixed, they would have created severe difficulties in an election with over 2,000 voters.

The locked clipboard worked poorly. It complicated and slowed down the process, made it difficult to drop ballots into the scanner, and added weight. Most voters felt it did not enhance security, despite its purpose of making it difficult to steal or swap ballots. At the scanning table, several voters mistakenly ripped their ballots off the locked clipboard. Technically, any ballot with torn locking hole was supposed to be invalid, but for simplicity this rule was not enforced.

Some elderly voters commented that they had difficulty reading the confirmation codes. Three voters reported that some confirmation codes blurred, especially if rubbed heavily, and one reported that the ballot paper deteriorated. On a positive note, marking the ballot with revealing ink produced perfectly darkened ovals: because there was no reactive ink outside the ovals, no darkening appeared there. Although this outcome was not the motivation for printing Scantegrity ballots with invisible ink, it appears evident that invisible ink yields a superior method for marking optical scan ballots. We supplied pointed "bullet" style special pens, to facilitate writing down the confirmation codes. Wider "chisel" style special pens, however, seem to work better for marking ovals.

Figure 7 shows correlations between survey responses on age and ease of use, and between understanding of Scantegrity and overall confidence in the system. As expected, overall, older voters found Scantegrity harder to use than did younger voters. Interestingly, most voters still had high confidence in Scantegrity, even if they felt they understood the system poorly. This finding runs contrary to a widely asserted notion that voters will not accept a system that they do not understand.

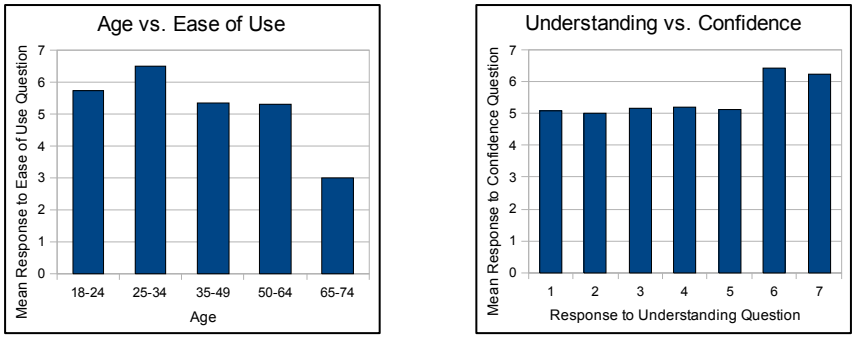


Figure 7. Correlation between age and overall ease of use, and between understanding and overall confidence in system. Voters under 65 years of age found Scantegrity easier to use. Voters who felt they understood the system very well had slightly higher confidence in the system, yet even those who felt they had a poor understanding of the system had a moderately high confidence in the system. Pearson correlation coefficients: age vs. ease of use: -0.20, understanding vs. confidence: 0.28. (1 = strongly disagree, 7 = strongly agree)

6 Recommendations

To simplify and streamline the process, we recommend the following:

1. Eliminate the locked clipboard.
2. Eliminate redundant instructions. At beginning of process, do not provide instructions for optional steps.
3. Use high-quality, fast, robust scanners—preferably of the type that automatically drops the ballot into the ballot box when the voter signals to cast the ballot. The scanner should accept ballots inserted in any orientation.
4. Add a printer to the scanner to provide a digitally signed receipt with the confirmation codes. Great care must be taken to ensure that this printer does not violate ballot privacy (Fink and Sherman [Fin09] suggest one approach).
5. Eliminate the tear-off chit. Instead, provide a separate sheet of paper to any voter who wishes to write down confirmation codes or other ballot information by hand.
6. Print confirmation codes with a restricted character set to avoid easily confused letters.
7. Use “chisel” style special pens for ease of marking ovals, selecting a small enough chisel width to permit writing down confirmation codes and write-in candidates.
8. Thoroughly analyze and test the voting process with many diverse voters.

7 Conclusions

The mock election demonstrated that Scantegrity can be effectively used in elections and is well accepted by voters. Survey data show that voters feel comfortable with the system and have confidence in it.

Mock1 revealed though that the flow of people through the voting process must be greatly improved. The implementation, procedures, voter instructions, and equipment of Scantegrity used in this election need to be simplified and streamlined. Although Scantegrity significantly simplifies the voting process from its predecessors SureVote and Punchscan, additional attention is needed to improve and fine tune the voter experience, including the physical processes of receiving, marking, and scanning the paper ballot.

After polls closed, thirty-one of the ninety-five voters verified their votes online, demonstrating that a sufficient number of voters will likely take advantage of the verification option in E2E systems. This percent of voters verifying their votes is consistent with that observed in our other Punchscan and Scantegrity trials. We conjecture, however, that in binding elections, the percentage will also depend on the degree of interest in and contention of the races.

Our findings include that the locked clipboard added complexity, but did not enhance security, and that revealing ink provides a superior technology for marking optical scan ballots with perfectly darkened ovals.

Even though many voters do not care much about security and tend to trust voting systems, a small and vocal group of political activists is very concerned about this issue. Deploying systems like Scantegrity fundamentally enhances outcome integrity and directly addresses those activists concerns.

Accessibility for voters with disabilities was not a focus of this study. In separate projects, our team is seeking better solutions for the vital challenge of making high-integrity voting truly accessible to differently-abled voters, including the blind.

Learning from Mock1, we implemented the following changes for the subsequent binding election: eliminated the locked clipboard, designed a new privacy sleeve, eliminated the monitor check at scanning, added a second scanner, built ballot feeders for the scanners, used a double-ended pen with chisel and bullet points, eliminated redundant instructions, improved signage and instructions at registration and in the voting booths, and used a separate receipt card rather than a tear-off chit.

Mock1 helped pave the way for Scantegrity's successful deployment in the November 2009 binding governmental election in Takoma Park [Car10]. Lessons learned from this feasibility demonstration helped streamline voter flow, reduce average voting time (from 8 min to 2.5 min), and improve instructions to voters.

8 Acknowledgments

We are grateful to the many people who made this pilot study of Scantegrity possible, especially Anne Sergeant (Chair, Takoma Park Board of Elections), other members of the Board, Jessie Carpenter (City Clerk), and the Mock1 voters. Lynn Baumeister led the focus groups and offered numerous practical suggestions. Brian Strege and Fahad Alduraibi observed voters. Russell Fink, Douglas Jones, Sharon Laskowski, and Svetlana Lowry provided useful feedback. Esther Haynes offered editorial suggestions.

Sherman was supported in part by the Department of Defense under IASP grant H98230-09-1-0404.

Vora and Popoveniuc were supported in part by National Science Foundation under SGER grant NSF-CNS-0831149.

Bibliography

[Adi09] Adida, B. *et. al*. 2009. Electing a university president using open-audit voting: analysis of real-world use of Helios. In *Online proceedings of EVT 2009* http://www.usenix.org/event/evtwote09/tech/full_papers/adida-helios.pdf

[Alv08] Alvarez, R. M., and E.T. Hall: 2008. Electronic elections: The perils and promises of electronic democracy. Princeton, NJ, USA: Princeton University Press.

[Bau09] Baumeister, L. 2009. Mock election notes: Mock election, April 11. Takoma Park.

[Bed03] Nederson, B. *et. al.* 2003. Electronic voting system usability issues. In *Proceedings of the SIGCHI conference on human factors in computing systems,* 145-152.

[Ben04] Bensel, R. F. 2004. The American ballot box in the mid-nineteenth century. New York: Cambridge University Press.

[Byr07] Byrne, M. D., K. K. Greene, and S. P. Everett. 2007. Usability of voting systems: Baseline data for paper, punch cards, and lever machines. In *Human factors in computing systems: Proceedings of CHI 2007,* 171-180. New York: ACM.

[Car10] Carback, R. *et al.* 2010. Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy, USENIX security 2010. http://www.usenix.org/events/sec10/

[Cha09] Chaum, D., et. al. 2009. Scantegrity: End-to-end verifiability for optical scan elections. In *IEEE Transaction on Information, Forensics, and Security - special issue on voting* 4 (4): 611-627.

[Con09] Conrad, F., *et. al*. 2009. Electronic voting eliminates hanging chads but introduces new usability challenges. In *International Journal of Human-Computer Studies* 67 (1): 111–124.

[Cra05] Cranor, L.; and S. Garfinkel S. 2005. Security and usability: Designing secure systems that people can use. O'Reilley.

[Ess07] Essex, A. *et. al*. 2007. Punchscan in practice: An E2E election case study. Proceedings of the IAVoSS workshop on trustworthy elections (WOTE 2007).

[Fin09] Fink, R., and A. T. Sherman A. T. 2009. Combining end-to-end voting with trustworthy computing for greater privacy, trust, accessibility, and usability (summary). In *Proceedings of the NIST workshop on end-to-end voting systems,* October 13-14.

[Her06] Herrnson, P. S. *et. al*. 2006. The importance of usability testing of voting systems. In *Proceedings of the USENIX/accurate electronic voting technology on USENIX/Accurate electronic voting technology workshop.* http://www.usenix.org/events/evt06/tech/full_papers/herrnson/herrnson.pdf

[Her08] Herrnson, P. S. *et. al*. 2008. Voting technology: The not-so-simple act of casting a ballot. Washington, DC: Brookings Institution Press.

[Hub05] Hubbers, E., B. Jacobs, and W. Pieters. 2005. RIES: Internet voting in action. In *Proceedings of the COMPSAC*.

[Las04] Laskowski, S. 2004. Improving the usability and accessibility of voting systems and products. NIST Special Publications SP 500-256.

[New08] Newkirk, G. M. 2008. Trends in American trust in voting technology, March 17, white paper. InfoSENTRY Services.

[OSCE07] Office for Democratic Institutions and Human Rights. 2007. The Netherlands parliamentary elections, 22 November 2006, OSCE/ODIHR election assessment mission report. Warsaw.

[Pou08] Poundstone, W. 2008. Gaming the vote: Why elections aren't fair (and what we can do about it). New York: Hill and Wang.

[Punch] Punchscan. http://www.punchscan.org/

[Scan] Scantegrity. http://www.scantegrity.org/

[ScaT] Takoma Park Election Day Scantegrity Website. http://www.scantegrity.org/takoma/

[She09] Sherman, A. T. 2009. Scantegrity mock election at Takoma Park (summary). In *Proceedings of the NIST workshop on end-to-end voting systems, October 13-14.*

[Shn05] Shneiderman, B., and C. Plaisant. 2005. Designing the user interface, 4th edition. Addison Wesley.

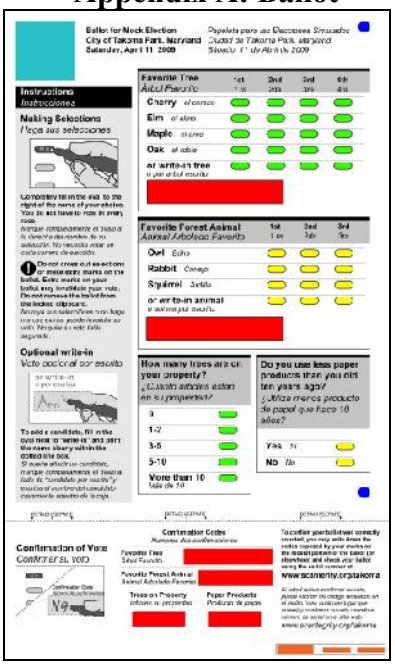
[Tako] City of Takoma Park. http://www.takomaparkmd.gov/

[TPN09] Takoma Park Newsletter. 2009. This Arbor Day: Plant the seeds for election verifiability. April.

[EAC05] United States Election Assistance Commission. 2005. Voluntary voting system guidelines. December.

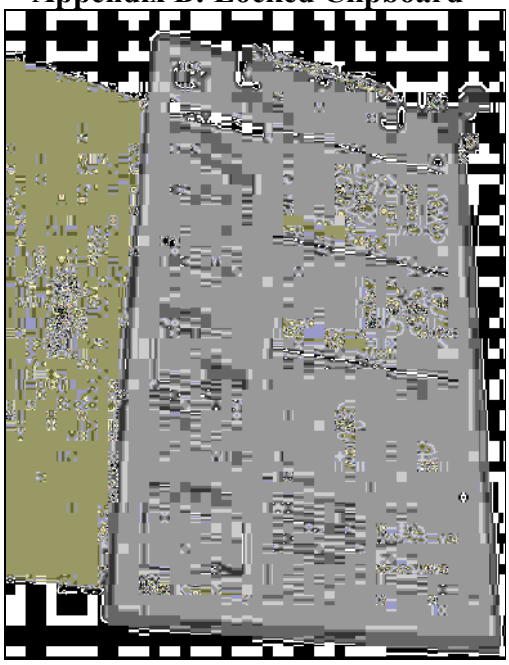
[Voc07] VoComp. http://www.vocomp.org/

Appendix A: Ballot



Ballot shown smaller than actual size.

Appendix B: Locked Clipboard



Locked clipboard resists chain voting.

Session 2: Sociocultural Issues of E-Voting

The role of trust, participation and identity in the propensity to e- and i-vote

Letizia Caporusso

Dipartimento di Sociologia e Ricerca Sociale
Università degli Studi di Trento
Via Verdi, 26
38122 Trento, Italy
letizia.caporusso@unitn.it

Abstract: The paper analyzes the issue of citizens' propensity to deploy automated elections as a dependent of several ascribed and attitudinal factors. Data are drawn from a computer-assisted telephone survey carried out in the Autonomous Province of Trento, which through project ProVotE sponsors the largest program of touchscreen-based voting in Italy. Alongside socio-demographic variables such as sex, age, education, and occupation, we describe how socio-political attitudes such as trust, participation, and identity affect the propensity to vote by automated means. We conclude that, based on the binomial and multinomial logistic models we implemented, our data support the hypothesis of existing divides between those who are favourable to automation in elections and those who are not, the main cleavages being age and level of education. Furthermore, a greater degree of trust in the generalised other is needed in e-voting but not perceived in i-voting, while both voting procedures appeal those who are already politically mobilized but less attached to traditions.

1 Introduction and research hypotheses

To the eyes of an external observer, the European electoral legislation landscape appears as a colourful and assorted patchwork of requirements, procedures, and technical tools. Some countries revoked e-voting as soon as they loss support from the electoral basis, no matter whether it was a novelty, as in Ireland [Co04a; Co04b; Co06; Lu07] or a long established habit, as in the Netherlands [Go06; Oo07]. Others are more cautious and promote trials and experimentations with or without legal value, but always on a limited scale: this is the case in Switzerland [Br04; BB06], Great Britain [FR03], Spain [Fe07], Portugal [Fa08], and Italy [Ca08]. Some countries, such as Belgium and France, currently deploy electronic machines, while a few Baltic explorers are adopting more and more innovative channels: i-voting, successfully deployed in Estonia [MM06] and debated in Lithuania [Ud06], and even m-voting, i.e., voting from a mobile phone, as recently approved in Estonia [Wo08].

For the purposes of this paper, it is necessary to distinguish between paper-and-pencil polling-place voting, which is the traditional solution adopted by the Italian legislation; electronic voting by means of a computer installed in voting booths that are not connected to any network, generally labelled as *e-voting*; and internet voting from unsupervised environments, known as RIV (Remote Internet Voting) or just *i-voting*.

E-voting generally reproduces the features of the paper ballot on a more advanced technological artefact, allowing for quicker tabulation of the results and preventing some kinds of clerical mistakes in filling in the different measures [Re04]. I-voting can be regarded as a form of absentee ballot involving a further evolutionary step of technological development and reproducing dynamics similar to those faced in mail-in balloting [PS08].

Though more and more salient in Europe and in the rest of the world, the sociological debate pro and versus automated voting rests primarily on theoretical basis. Some authors underline how electronic voting will revolutionize democracy for the better by reducing costs, by limiting errors made by voters and electoral administrators, but above all by allowing for uniform standards in the ballot format [SC05]. Besides, thanks to an immediate access to online sources of information, i-voters could express a more documented and informed choice [AH04]. Conversely, other commentators believe that by making voting too easy and convenient, one would actually diminish the percentage of voters who really care about a certain policy; therefore e- and i-voting do not substantially revolutionize democracy [Bu01]. What is more, casting a ballot online is an individual business, which might deprive balloting of its symbolic value, which is intrinsically communitarian: all men and women—regardless of their age, status, education—walk as equals into anonymous polling booths and, as equals, decide to participate in the nation's destiny. Authors wonder whether democracy as we know it can be thus individualised and removed from its public expression. Opinions, again, are divided: some believe citizens are ready to give up the liminal phase of walking into the booth [Mo06], others see it as a betrayal of the democratic traditions and standpoints [MS04; Or01], the use of the internet apparently increasing social isolation [NE00]. In addition to this, as we already anticipated, the overall quality of democracy might be seriously affected by the divide in the access to automated voting facilities, which tend to be preferred by already mobilized social groups [Ke05], though this viewpoint is being fiercely debated [PS08]. Overall, electronic and internet voting appear as a promising challenge as much as a deceitful means supported by politicians to represent themselves as "modern" [FR03].

As a consequence, an oft debated topic is, at the time being, whether electronic and internet voting might change the socio-demographic and ideological profile of the electorate by facilitating some already advantaged social groups and discriminating the minorities. Some characteristics of the population have been proved to be associated with the ability of voting with different technologies: for instance, the amount of residual votes on ballot measures is linked to the voting technologies alongside the income and the percentage of black people living in a given county, whereas age and the percentage of Latinos appear to be not significantly associated to the chosen procedure [KK08]. Similar considerations might apply to the introduction of an electronic medium to replace a long-established habit of voting by paper and pencil.

Legally binding i-voting experiences show contradictory results: surveys conducted after the Arizona democratic primary in 2000 converge on finding a significant impact of age and level of education, whereas sex should not play a role in the choice to vote online [Ke05; So01]. On the other side, they substantially diverge in their interpretation of the effect of income, which is significant at the bivariate level [Ke05; So01] or when crossing ecological rather than individual data [Gi01], but looses its power when pooled in a multivariate model [So01]. Location (urban/rural) would not exert a statistically

significant effect [So01], as well as party identification [Ke05]. While some authors insisted on the existence of a digital divide between different social classes, sex and age groups [Gi05], individual level turnout data from the 2004 Michigan democratic primaries allowed researchers to signally address campaigners' concerns. Race and class were not found to be significant and a two-step decision model clarified that their impact is limited to the choice of voting absentee: once this decision has been taken, they play no role on the selection of the preferred method (by mail or by internet) to cast the ballot [PS08].

We can therefore expect sex, age, occupation, and education to be associated with the propensity to vote over the internet or on-site, by electronic means.

Furthermore, potential disparities might be observed not just in terms of the socio-demographic composition of the e-/i-electorate, but also in its quality: sociologists and political scientists are interested in observing how much an individual is linked to her socio-political community, and whether different modes of relation between a citizen and the society might affect her interest in e- and i-voting.

As pointed out by Guerra et al. [Gu03], trust in the other is crucial in establishing relations, and it has been argued that the trust flow starts with trust in the institutions delivering the elections [XM05]. It has also been underlined that i-voting will advantage citizens of areas where political participation is higher [Bi05], i.e., will appeal those who are already mobilized [KK08]. The bivariate association between political efficacy and willingness to vote over the internet has been established by Solop [So01], though he did not specify how the index is calculated, nor control for socio-demographic variables. A further condition supporting the deployment of automated means is the sense of belonging to the community, a concept which has been referred to as "social identity" [OV05], though not implying the identification of the individual by others, as intended by Guerra et al. [Gu03], but rather the feeling of describing oneself as part of a meaningful social group.

Given these premises, we might expect that trusting institutions and the generalised other, feeling as a member of one's community, and taking part in political activities beyond voting might increase the chances of being in favour of electronic and internet balloting.

The analysis that follows will then address the following question: what circumstances—socio-demographic characteristics and political attitudes—are associated with the (un)willingness to cast one's ballot from a terminal?

2 Data and methods

Since December 2004, the Autonomous Province of Trento has sponsored a research plan aimed at investigating and supporting the transition to automated means of casting and counting ballots in local elections. Pilots took place in 2005, 2006, and 2008 within the largest project of electronic voting carried out in Italy so far. The local government deployed a phased-in approach as suggested, among others, by the European Commission [Ve04], with the goal of gradually substituting paper and pencil with touchscreens. At the time this paper was being written, the multi-disciplinary *équipe* working on the ProVotE project provided local authorities with detailed evaluations of the field trials and recommendations on the conditions under which the switch-over

should take place, but no final decision has been taken yet. As none of the pilots could be legally binding, and individual-level data of voters and non-voters are not available, we relied on surveys to monitor the propensity to vote electronically in a supervised environment and over the internet (as done previously, amongst others, by Gibson [Gi01] and Kenski [Ke05]). Although i-voting is not on the agenda of either the Italian government or of the local one, the growing salience of this topic in the international arena suggested that we should start a preliminary investigation in order to highlight the conditions underlying the support for and the opposition against it.
Data that will be presented in this contribution are drawn from computer assisted telephone interviews carried out at the beginning of December 2007 on a sample of 1603 adult citizens. The sample was stratified in order to be representative of sex, age, and town of residence.

The three dependent variables reflect:
- the interviewee's propensity to deploy ProVotE e-voting machine (model a),
- the general stereotype towards automated voting, i.e., whether it has more advantages or more risks (model b), and
- the propensity to vote over the internet (model c).

These three variables were dichotomized by collapsing answers that expressed favor in the new technology and those that did not, as shown in Table 1.

As independent variables, we considered a set of socio-demographic characteristics (sex, age, level of education, and type of occupation) but also some indexes[1] of social and the political attitudes that the above summarized literature review held as theoretically or empirically crucial.
Specifically, an index of *trust in the generalised other* was computed from three dichotomous items following the Survey Research Center's rephrasing of Rosenberg's Faith in People scale [RS85], which is still being deployed in its ten point version in the European Social Survey. Given the limited number of items available, we did not compute a quasi-cardinal measure but rather aggregated the answers in order to separate those who tend to trust others (60.5% of valid cases) from those who offer no positive answer (39.5%). Bivariate analysis showed that education is the most significant factor related to this attitude: people in their adult age tend to trust others more than youth and the elderly. Bourgeois are more confident than interviewees of the working class, whereas sex has no significant impact.
In order to tap beliefs about politicians and the political process, we computed an index of *political cynicism*[2] by adapting Agger, Goldstein, and Pearl's scale [AGP61]. This quasi-cardinal measure is positively correlated to age and negatively correlated to the level of education, whereas there is no significant difference between sexes and occupations.

[1] A full list of the items enclosed in the survey is available upon request.
[2] Given the nature of the data gathering method (CATI), we offered just five modes of response instead of the original six. The standardised index has been computed using five of the six items, thus obtaining good internal consistency (Crombach's $\alpha = 0.63$). The median is 0.24, skewness is -0.566, kurtosis is 0.720 and range is 6.266.

A further index of *trust in the local institutions*[3] was computed by translating Craig, Niemi, and Silver's incumbent-based trust scale [CNS90], supplementing it with two items from Bennett's governmental attentiveness scale and ANES studies [RSW91], and adapting their wording for the local dimension. This attitude is actually cross-sectional and unrelated to sex, age, education, and occupation.

A second crucial dimension, *political participation*[4], is represented by political activities: an index was computed from nine dichotomous items deployed within the Italian National Election Study [It06] and Verba and Nie's Participation in America Survey [Br99].

Voting in the last general election was retained as a separate control variable: 86.7% of the respondents declared they voted, an estimate which is consistent with the turnout of 2006 political elections in the region Trentino-Alto Adige, where the recorded participation rate was 87% [Mi09].

The third social dimension taken into consideration is the feeling of *territorial identity*, the sense of belonging to a local community that shares the same heritage and identifies itself in both symbols and actions. The indicators chosen to elicit this concept were only in part inspired by ANES studies and adapted to the local reality, so the resulting typology is original and not yet tested for external validity. We distinguished five types of interviewees:

- enthusiastic (26.4%) are proud of whatever concerns their land, possibly even edging toward chauvinism. Within this group women are more represented than men, as well as lower grades of education and people over their fifties;
- un-socialised (17.0%), though they define themselves as "trentini", they do not know the anthem, which is usually taught at school and sung at local festivities. As just one out of four was born outside the province, it is likely that people within this group are less integrated than those providing on-average or even enthusiastic answers. More women than men belong to this type, and seven out of ten are below fifty years of age;
- disillusioned (10.2%) said they feel little attached to at least one of the symbols taken into consideration. Disillusion is more common amongst young men and higher-grade white collars;
- strangers (11.0%) declared they do not feel themselves to be citizens of the Autonomous Province of Trento, or didn't answer to the identity-related questions. Interestingly, this attitude is more common amongst middle-aged professionals and those with higher education level: no surprise that just one out of four was born in the province;
- the remaining 35.4% gave intermediate answers and were labelled as "middlemen".

Given the nature of the dependent variables, we deployed multinomial and binary logistic regression and report the regression parameters (B), their Wald test significance

[3] In its original version this scale was deployed with dichotomous items, while our version has five possible answers. The index is standardised, with median of 0.08, skewness -0.007, kurtosis -0.302, and range 6.002.

[4] The summation index has been standardised and has a median of 0.13, skewness 0.683, kurtosis 0.052, range 4.654. The resulting Crombach's alfa is 0.64.

and their standard errors. Odds ratios can be easily computed by raising the base of the natural log to the B^{th} power.

Table 1 – *Propensity towards the automation of voting procedures*

a. Propensity to e-vote	%	b. Electronic voting has…	%	c. Propensity to i-vote	%
very much in favour	25.8	more advantages than risks	36.3	very much in favour	16.0
quite in favour	30.0	more risks than advantages	35.7	quite in favour	23.9
neither in favour nor against	11.6			a little/not much in favour	17.5
quite against	14.7			not at all in favour	36.6
very much against	11.8				
Total valid cases	*93.9*	*Total valid cases*	*72.0*	*Total valid cases*	*93.9*
did not answer	0.4	did not answer	0.3	did not answer	0.2
did not know	5.7	did not know	27.7	did not know	5.9
Total	*100.0*	*Total*	*100.0*	*Total*	*100.0*
N	*1603*	*N*	*1603*	*N*	*1603*

3 Discussion of the results

Consistently with the reviewed literature on cyber-trust, remote i-voting elicits less support than polling-place e-voting: the latter is approved by 55.8% of the interviewees, whereas the former by 39.9% [Table 1]. The data support the hypothesis of an incremental deployment of technology, which sees e-voting as a step in an evolutionary process in which paper and pencils yield to remote internet voting: there is just a limited amount of respondents who would accept i-voting but not e-voting (3.7%), likely because of the added value of voting remotely rather then by the deployment of technology [Table 2].

But what is the profile of voters who would support automated elections? How much do socio-demographic characteristics affect the propensity to vote on a touchscreen or over the internet? Is there an impact of socio-political attitudes on this choice?

Table 2 – *Attitudes towards different solutions for voting automation*

%	a. Propensity to e-vote			b. Propensity to i-vote		
Electronic voting has…	no	yes	Total	no	yes	Total
more advantages than risks	29.7	17.0	46.7	38.1	12.1	50.1
more risks than advantages	3.5	49.8	53.3	16.9	32.9	49.9
Total	33.2	66.8	100.0	55.0	45.0	100.0
	r =.603 (sig=.000)		*N=1021*	*r =.422 (sig=.000)*		*N=1111*

%	c. Propensity to e-vote		
Propensity to i-vote	no	yes	Total
no	29.0	25.3	56.4
yes	3.7	42.0	43.6
Total	32.7	67.3	100.0
	r =.482 (sig=.000)		*N=1260*

3.1 Socio-demographic characteristics

The analysis carried out by means of a multivariate logistic regression model allows us to compare the characteristics of those who answered favourably, those who are against, and those who provided no opinion on the subject matter, which gives us some insight into the potential non-response bias affecting surveys on e- and i-voting [Table 3]. We thus observe that interviewees who do not take a stand on the issues are also less likely to provide personal details, especially with regard to their occupation, while missing information on age is related to missing information on i-voting.

The model also shows that sex impacts significantly on the chances to see more risks than advantages in automated voting, but women are more sceptical than men also with reference to the ProVotE stand-alone machine and to i-voting. Age has a non-linear effect: consistently with previous research (e.g., Gibson [Gi05]) we find that automated elections are more supported by people in their middle age than by the youngsters and the elderly. The level of education contributes to the interest for these innovations in the electoral procedures: all factors being equal, the chances that a graduate supports i-voting are nearly twice as much as those of a person with a lower degree. Finally, there is no direct effect from occupation, which nonetheless is retained in the following analysis as a control variable.

Table 3: *Effects of socio-demographic characteristics on the propensity to automation in electoral procedures*

	a. Propensity to e-vote				**b.** Electronic voting has more advantages				**c.** Propensity to i-vote			
	yes		**indifferent / DA / DK**		**yes**		**DA / DK**		**yes**		**DA / DK**	
	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE
Sex												
male	0.15	0.123	-1.08	0.788	0.46***	0.122	0.13	0.132	0.20	0.112	0.13	0.224
female [a]												
Age												
missing	1.06	0.671	1.08	0.788	1.02	0.770	1.31	0.697	1.63*	0.641	2.17*	1.063
age	0.07***	0.020	0.02	0.025	0.05**	0.021	-0.01	0.021	0.08***	0.020	0.05	0.036
age*age	-0.01***	0.001	-0.01	0.001	-0.00**	0.000	0.01	0.001	-0.01***	0.000	-0.01	0.000
Education												
missing	0.02	0.864	0.20	0.978	0.40	1.049	0.45	0.934	0.07	0.902	-0.30	1.197
min. 4 yrs univ. degree	0.64*	0.301	0.36	0.402	0.82**	0.310	-0.61	0.342	1.26***	0.303	-1.48	0.812
high school / BA	0.75**	0.234	0.76**	0.288	0.57*	0.256	-0.09	0.242	0.90***	0.255	-0.40	0.386
mid. school / prof. educ	0.39	0.214	0.65*	0.257	0.22	0.243	0.11	0.217	0.37	0.247	0.01	0.330
no title / elem. school [a]												
Occupation												
missing	-0.01	0.212	0.50*	0.251	0.26	0.225	0.48*	0.218	-0.13	0.214	0.67*	0.326
bourgeoisie	0.27	0.277	-0.56	0.448	-0.22	0.264	-0.41	0.325	0.53*	0.252	0.01	0.645
petite bourgeoisie	0.37	0.221	0.41	0.278	0.22	0.214	0.26	0.227	0.30	0.195	-0.09	0.423
white collars. high skilled	0.16	0.193	0.32	0.250	-0.14	0.190	0.32	0.201	0.08	0.172	0.36	0.353
white collars. low skilled	-0.07	0.184	0.16	0.238	0.28	0.184	0.22	0.202	0.26	0.170	0.53	0.320
working class [a]												
Constant	-1.27*	0.492	-1.87**	0.632	-1.81	0.508	-0.90	0.524	-2.25***	0.490	-3.52***	0.944

[a] reference category. Multinomial logistic regression models. DA = does not answer; DK = does not know. *p < .05 **p < .01 ***p < .001

model a.: N=1603. Model $\chi^2(df)^{sig}$ = 122.192(26)***. –2LL = 2530.168; Pseudo R^2: Cox&Snell = 0.073, Nagelkerke = 0.085, McFadden 0.039.

model b.: N=1603. Model $\chi^2(df)^{sig}$ = 140.702(26)***. –2LL = 2628.343; Pseudo R^2: Cox&Snell = 0.084, Nagelkerke = 0.095, McFadden 0.040.

model c.: N=1603. Model $\chi^2(df)^{sig}$ = 224.639(26)***. –2LL = 1976.318; Pseudo R^2: Cox&Snell = 0.131, Nagelkerke = 0.159, McFadden 0.081.

3.2 Social and political attitudes

To ascertain the role of the three socio-political dimensions described in section 2 (trust, participation, identity), we ran different binomial logistic models and found that the sign, the magnitude, and the significance of the coefficients did not substantially differ from what we observed in a single all-encompassing model, which is presented in Table 4.

Within the first dimension, we expected that *trust in the generalised other*—as a feeling that contrasts with, for instance, complot theories—would enhance the chances to accept automated elections. All other factors being held constant, this index was found to be relevant as long as voting in a supervised environment is concerned (model a and b) but negligible in the i-voting model. A possible interpretation of this result might take into account the relative safety of the voting environment as perceived by the elector: whereas automated voting as presented in the first two questions can be easily prefigured as quite similar to the present way of casting a ballot—where the computer takes over the paper and pencils—the third question suggests a totally different and much individualised location. The generalised other then is not the technician, the programmer, distant, invisible and perhaps even transparent to the eyes of the voter, but she is rather the returning officer, the member of the board of the scrutinizers, who support the elector in exerting her right to vote.
Political cynicism does not have much impact on the prejudice against automated voting (does it have more risks or more advantages) nor on the imaginary of remote voting, but rather it does on its practical application: interestingly enough, the cynical elector welcomes ProVotE, likely as a possible solution to potential frauds at the very local level. A large scale complot, as envisioned by activists in other countries with regard to i-voting, seems not to be foreseen by our interviewees.
Finally, we found no support for the common rhetoric that holds automated voting as better accepted by citizens who trust the local government. Controlling for all other socio-demographic and socio-political factors, *trust in the local administration* appears to be cross sectional: the coefficients are weak and non significant, though the sign of the relationship is consistent with our research hypothesis.

The second dimension we considered is *political participation*, which encompasses a set of political actions, such as signing up for a petition or a referendum, writing to candidates, trying to convince someone to vote for a party and so on. Our data bring further evidence to an already consolidated literature stressing how e- and i-voting appeal to citizens who are already politically mobilized. But we also found a small effect related to voting in past elections: those who did not cast a ballot have more chances to be in favour of automated means and especially remote voting appears significantly attractive. These results support what we already anticipated: the attraction of this innovation is given by the possibility to vote comfortably from an individually chosen location rather than by the deployment of technology *tout court*.

Table 4: *Effects of socio-political attitudes on the propensity towards voting automation*

	a. Propensity to e-vote		b. Electronic voting has more advantages		c. Propensity to i-vote	
	B	SE	B	SE	B	SE
Sex						
male	0.17	0.127	0.47***	0.125	0.20	0.114
female [a]						
Age						
missing	1.03	0.706	1.12	0.845	1.64*	0.664
age	0.07**	0.021	0.05*	0.022	0.07***	0.021
age*age	-0.01***	0.001	-0.01*	0.001	-0.01***	0.000
Education						
missing	-0.31	0.895	0.22	1.178	-0.11	0.913
min. 4 yrs university degree	0.56	0.317	0.76*	0.321	1.02**	0.311
high school / BA	0.69**	0.243	0.53*	0.263	0.75**	0.260
middle school / professional edu	0.35	0.221	0.20	0.248	0.30	0.250
no title / elementary school [a]						
Occupation						
missing	-0.01	0.220	0.29	0.234	-0.19	0.220
bourgeoisie	0.14	0.283	-0.30	0.273	0.49	0.258
petite bourgeoisie	0.29	0.228	0.14	0.221	0.24	0.199
white collars. high skilled	0.11	0.200	-0.22	0.196	0.05	0.177
white collars. low skilled	-0.13	0.189	0.27	0.189	0.26	0.173
working class [a]						
Trust						
missing trust in the other	0.34	0.180	0.42*	0.183	0.01	0.165
trust in the other	0.53***	0.141	0.65***	0.141	0.248	0.132
missing political cynicism	-0.11	0.160	-0.03	0.166	0.15	0.149
political cynicism	0.15*	0.073	0.05	0.071	0.06	0.066
missing trust in local gov.	-0.08	0.142	-0.02	0.144	-0.21	0.133
trust in local government	0.08	0.078	0.05	0.074	0.06	0.069
Political participation						
missing political activities	0.81**	0.276	0.45	0.253	0.28	0.215
political activities	0.18*	0.070	0.06	0.069	0.27***	0.063
missing voting	-0.33	0.480	-1.15	0.638	0.12	0.441
voting in last elections	-0.14	0.209	-0.20	0.203	-0.35	0.189
Territorial identity						
enthusiastic	-0.11	0.233	-0.15	0.227	-0.35	0.208
middlemen	-0.20	0.224	-0.14	0.217	-0.30	0.197
disillusioned	-0.50	0.272	0.27	0.268	-0.25	0.241
un-socialised	0.12	0.248	0.16	0.237	-0.06	0.217
strangers [a]						
Constant	-1.28*	0.563	-1.94**	0.578	-1.71**	0.543

[a] reference category. Binomial logistic regression models. *$p < .05$ **$p < .01$ ***$p < .001$

model a.: N=1319. Model $\chi^2(df)^{sig}$ = 119.025(27)***. –2LL = 1537.538;
Cox&Snell R^2 = 0.086, Nagelkerke R^2 = 0.121. Overall % of predictability = 70.7%
model b.: N=1154. Model $\chi^2(df)^{sig}$ = 84.499(27)***. –2LL = 1515.616;
Cox&Snell R^2 = 0.071, Nagelkerke R^2 = 0.094. Overall % of predictability = 59.1%
model c.: N=1505. Model $\chi^2(df)^{sig}$ = 228.520(27)***. –2LL = 1822.873;
Cox&Snell R^2 = 0.141, Nagelkerke R^2 = 0.199. Overall % of predictability = 65.7%

The last dimension under analysis concerns the operationalization of identity according to the typology described in section 2. Though not statistically significant (which might be due, amongst other reasons, to the sample size), the sign and the magnitude of the coefficients suggest us some ideas about the effect of identity on the propensity to deploy automated means for voting. Quite interestingly, people who are more integrated in their community are less inclined to e- and i-voting: a conservative or traditionalist attitude, the pride of belonging to the community (though the same one which crafted the voting device) do not reinforce the willingness to vote automatically, but rather inhibit it. This finding goes in the opposite direction of our initial research hypothesis, according to which we expected that being a protagonist of such an innovation would be associated with a higher propensity to deploy the ProVotE machinery, in a sort of Hawthorne

factory effect [Ma33]. We can try to interpret this tendency in the light of the Durkheimian notion of community, which requires the members' co-presence in order to elicit, through rituals, that feeling of effervescence that recalls and forwards the shared values and norms.

4 Conclusions

The governments' preoccupation with the increasing disenfranchisement of the electorate brought about numerous attempts to restore citizens' participation in elections. Alongside reforms in the traditional paper-based electoral systems, many countries show a growing interest in automated means for casting ballots and tabulating the results. Automated elections promise a simplification of procedures, thus eliminating voters' fatigue (which is one of the causes of undervoting), clerical mistakes, and, possibly, low turn-out [KK08]. Nonetheless at the time being, empirical evidence is scarce if not anecdotal: literature draws on different sources of data and contexts that do not allow generalization.

Rather than on certainties on the feasibility and the advantages of e- and i-voting, most national experiences converge on the preoccupations advanced by pressure-groups and by some researchers: do automated elections change the composition of the electorate and thus the quality of democracy?

Our data showed that age and education level are significant predictors of the propensity to vote remotely or in electronic booths, the effect of age being actually non-linear, thus suggesting that youth, as well as the elderly, will not be attracted to polls, should e-voting be introduced, neither will people with low levels of education.

But we also considered how the voters' profile will change according to their socio-political attitudes, signally with reference to trust, political participation, and identity.

We found further evidence to Xenakis' and Macintosh's [XM05] suggestion that in the chain of inherited trust, citizens do not realize they implicitly give credit to someone who is unknown, not just to them, but even to the same authorities delivering the elections. I-voting propensity is actually unrelated to both trust in the local government and trust in the generalised other; in other words prospect i-voters experience different kinds of concerns than those sensed in other e-transactions, while trust in the other is significant when voting in a supervised environment. Our data therefore support Oostveen's and Van den Besselaar's statement, according to which "people should not just have to trust in the integrity of a voting system or the people who designed, developed and implemented it" [OV04], thus implying that more observation opportunities might be introduced to enhance the feeling of security. It is then advisable that on one side citizens should be enabled and encouraged to observe procedures at the polling booths, but on the other side they should also be made aware of the role of technology (and of the people in charge of designing and managing it) should i-voting be introduced.

Furthermore, as participation in political activities proved significant for both e- and i-voting, our data suggest that in the Italian context, and signally in Trentino, the conclusions drawn by Prevost and Schaffner [PS08] cannot be totally corroborated: if mobilization only influences the choice to vote remotely, but not the medium through which the ballot is cast, we should not have found political participation to be a

significant predictor in the e-voting model as well. We can therefore conclude that there is a substantial divide in the propensity to deploy automated means of elections: people who are already politically mobilized are more in favour of automated elections–as suggested, amongst others, by Kimball and Kropf [KK08], Kenski [Ke05], Birdsall [Bi05]–no matter whether voting takes place from a remote location or in a supervised environment. Nonetheless, we also found evidence that automated voting, especially in its i-form, might appeal those who did not participate in the last political elections.
Finally, we learnt that even though most i-voting initiatives have been developed at the local level by local contractors [Kr08], pride for belonging to the same community that crafted this innovation does not enhance the chances of being in favour of deploying the i-voting mechanisms, but on the contrary, a higher degree of integration inhibits the propensity to i-vote. We tried to interpret this attitude with reference to the Durkheimian theory of collective effervescence, which is elicited by ritual events such as elections.
The seeming contradiction between the positive impact of political participation and the negative, though not significant, impact of integration is a paradoxical finding that calls for further research. It is likely that mobilization is not disjoined from progressive individualization of conventional political behaviours, which would account for both the positive effect of participation and the irrelevant effect of integration, but a more complex model is needed to account for these relations, which goes far beyond the scope of this paper. Further investigations are also needed in the direction of the feeling of security and privacy that different media convey: for instance, how i-voting will eventually overcome the tension between the need for privacy and the requisite of identity recognition is still to be ascertained. We also acknowledge the limitations related to the method of data gathering we deployed: should similar data be available in real experimental settings, we will be able to confirm whether attitudes towards e- and i-voting match with actual behaviours or not. The next steps of our analysis will signally address the effect of the technological artefact and take into consideration the voters experience with current voting procedures and with technology in general, through scales that can be computed within the same dataset presented here.
At the time being, our research suggests that greater attention should be paid to the quality of the electorate that e- and i-vote engage: based on the binomial and multinomial logistic models we implemented, our data support the hypothesis of existing divides between those who are favourable to automation in elections and those who are not, the main cleavages being represented by age and education, but also by socio-political attitudes.

5 Acknowledgements

The author acknowledges that the research presented in this contribution was carried out within the project ProVotE, financed by the Autonomous Province of Trento, and wishes to thank the director of the Electoral Bureau, Patrizia Gentile, and the members of the sociological *équipe*—Carlo Buzzi, Francesca Sartori, Pierangelo Peri, and Giolo Fele—for their constant support and encouragement.

Bibliography

[AGP61] Agger, R. E., M. N. Goldstein, and S. A. Pearl. 1961. Political cynicism: Measurement and meaning. *Journal of Politics* 23: 477–507.

[Al06] Allen, P. L. 1906. Ballot laws and their workings. *Political Science Quarterly* 21: 38–58.

[AH04] Alvarez, R. M., and T. E. Hall. 2004. *Point, click, and vote. The future of Internet voting*. Washington, DC: Brookings Institution.

[Bi05] Birdsall, S. 2005. The democratic divide. *First Monday* 10. http://131.193.153.231/www/issues/issue10_4/birdsall/index.html

[Br99] Brady, H. E. 1999. Political participation. In *Measures of political attitudes*, ed. J. P. Robinson, P. R. Shaver, and L. S. Wrightsman, 737–801. San Diego, California: Academic Press.

[Br04] Braun, N. 2004. E-voting: Switzerland's projects and their legal framework. In *Electronic voting in Europe: Technology, law, politics and society*, ed. A. Prosser and R. Krimmer. 43-52. Bonn: GI.

[BB06] Braun, N. and D. Brändli 2006. Swiss e-voting pilot projects: Evaluation, situation analysis and how to proceed. In *Electronic voting 2006, GI lecture notes in informatics*, ed. R. Krimmer. 27-36. Bonn: GI.

[Bu01] Buchstein, H. 2001. Modernisierung der Demokratie durch e-Voting? *Leviathan: Zeitschrift fur Sozialwissenschaft* 29: 147–155.

[Ca08] Caporusso, L. 2008. There is more to e- than meets the eye: Towards automated voting in Italy. In *E-voting: The last electoral revolution*, ed. J. M. Reniu. 27-44. Barcelona: ICPS.

[Co04a] Commission on Electronic Voting. 2004. *First report of the Commission on Electronic Voting on secrecy, accuracy and testing of the chosen electronic voting system.* http://www.cev.ie/htm/report/download_first.htm

[Co04b] Commission on Electronic Voting. 2004. *Interim report of the Commission on electronic voting on secrecy, accuracy and testing of the chosen electronic voting System*. http://www.cev.ie/htm/report/V02.pdf

[Co06] Commission on Electronic Voting. 2006. *Second report of the Commission on electronic voting on secrecy, accuracy and testing of the chosen electronic voting system*.

[CNS90] Craig, S. C., R. G. Niemi, and G. E. Silver. 1990. Political efficacy and trust: A report on the NES pilot study items. *Political Behavior* 12: 289–314.

[FR03] Fairweather, B., and S. Rogerson. 2003. Internet voting—Well at least it's modern. *Representation* 39: 182–195.

[Fa08] Falcão, J. et al. 2008. Auditing e-voting pilot processes and systems at the elections for the European Parliament and for the Portuguese Parliament. In *E-voting: The last electoral revolution*, ed. J. M. Reniu. 93-114. Barcelona: ICPS.

[Fe07] Fernández Rodríguez, J. J. et al. 2007. *Voto electrónico. Estudio comparado en una aproximación juridico-politica (desafios y posibilidades)*. Santiago de Querétaro, Mexico: Fundación Universitaria de Derecho, Administración y Política.

[Gi01] Gibson, R. 2001-2. Elections online: Assessing internet voting in light of the Arizona democratic primary. *Political Science Quarterly* 16: 561–583.

[Gi05] Gibson, R. 2005. Internet voting and the European Parliament elections: Problems and prospects. In *The European Union and e-voting: Addressing the European Parliament's internet voting challenge*, ed. A. Trechsel and F. Mendez. London: Routledge.

[Go06] Gongrijp, R. et al. 2006. Nedap/Groenendaal ES3B voting computer. A security analysis, Stichting "Wij vertrouwen stemcomputers niet", Amsterdam. http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf

[Gu03] Guerra, G. A. et al. 2003. *Economics of trust in the information economy: Issues of identity, privacy and security*. Oxford: Oxford Internet Institute.

[It06] Itanes. 2006. http://www.itanes.org/.

[Ke05] Kenski, K. 2005. To i-vote or not to i-vote? Opinions about internet voting from Arizona voters. *Social Science Computer Review*.23:293-303

[KK08] Kimball, D. C., and M. Kropf. 2008. Voting technology, ballot measures, and residual votes. *American Politics Research* 36: 479–509.

[Kr08] Krimmer, R. 2008. The development of remote electronic voting in Europe. In *E-voting: The last electoral revolution*, ed. J. M. Reniu, 13–26. Barcelona: ICPS.

[Lu07] Lundell, J. 2007. Second report of the Irish Commission on electronic voting. *Voting Matters* 23: 13–17.

[MM06] Madise, Ü.,, and T. Martens. 2006. E-voting in Estonia 2005. The first practice of country-wide binding internet voting in the world. In *Electronic voting 2006, GI lecture notes in informatics*, ed. R. Krimmer. 15-26. Bonn: GI.

[MS04] Marvin, C., and P. Simonson. 2004. Voting alone: The decline of bodily mass communication and public sensationalism in presidential elections. *Communication and Critical/Cultural Studies* 1: 127–150.

[Ma33] Mayo, E. 1933. The human problems of an industrial civilization. New York: MacMillan.

[Mi09] Ministero dell'Interno, Archivio Storico delle Elezioni, 2009. http://elezionistorico.interno.it/

[Mo06] Monnoyer-Smith, L. 2006. How e-voting technology challenges traditional concepts of citizenship: An analysis of French voting rituals. In *Electronic voting 2006, GI lecture notes in informatics*, ed. R. Krimmer, 61–68. Bonn: GI.

[NE00] Nie, N. H., and L. Erbring. 2000. *Internet and society. A preliminary report*. Standford: Stanford Institute For The Quantitative Study Of Society. http://www.stanford.edu/group/siqss/Press_Release/Preliminary_Report.pdf/..

[Oo07] Oostveen, A.-M. 2007. Context matters. A social informatics perspective on the design and implications of large-scale e-government systems. Amsterdam: Universiteit van Amsterdam.

[OV04] Oostveen, A.-M., and P. Van den Besselaar. 2004. Security as belief. User's perceptions on the security of electronic voting systems. In Electronic voting in Europe: Technology, law, politics and society, ed. A. Prosser and R. Krimmer, 73–82. Bonn: GI.

[OV05] Oostveen, A.-M., and P. Van den Besselaar. 2005. Trust, identity and the effects of voting technologies on voting behavior. *Social Science Computer Review*..23: 304-311.

[Or01] Ornstein, N. 2001. What does the law require? Panel 4: Perspectives of political parties, 3rd public hearing of the national commission on election reform, held on May 24, 2001, in Austin, Texas.

[PS08] Prevost, A. K., B. F. Schaffner. 2008. Digital divide or just another absentee ballot?: Evaluating internet voting in the 2004 Michigan democratic primary. *American Politics Research* 36: 510–529.

[Re04] Remmert, M. 2004. Toward European standards in electronic voting. In Electronic voting in Europe: Technology, law, politics and society, ed. A. Prosser and R. Krimmer. 13-16. Bonn: GI.

[RS85] Robinson, J. P. and P. R. Shaver, eds. 1985. *Measures of social psychological attitudes*. Ann Arbor, Michigan: University of Michigan, Institute for Social Research.

[RS91] Robinson, J. P., P. R. Shaver, and L. S. Wrightsman, eds. 1991. Measures of personality and social psychological attitudes. San Diego, California: Academic press.

[SC05] Smith, A. D., and J. S. Clark. 2005. Revolutionising the voting process through online strategies. *Online Information Review* 29: 513–530.

[So01] Solop, F. I. 2001. Digital democracy comes of age: Internet voting and the 2000 Arizona democratic primary election. *PS: Political Science & Politics* 34: 289–293.

[Ud06] Udris, J. 2006. The Lithuanian concept of voting via internet for elections and referenda. Presentation held at the Council of Europe on account of the Central Electoral Commission of the Republic of Lithuania, November 16, in Strasbourg, France.

[Ve04] Venice Commission. 2004. Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe. In *European Commission for democracy through law*. http://venice.coe.int/

[Wo08] World E-Democracy Forum. 2008. Estonia to vote by mobile phone in 2011. http://www.edemocracy-forum.com/2008/12/estonia-to-vote-by-mobile-phone-in-2011.html

[XM05] Xenakis, A., and A. Macintosh. 2005. Trust analysis of the UK e-voting pilots. *Social Science Computer Review* 23: 312-325..

The Virtual Polling Station
Transferring the Sociocultural Effect of Poll Site Elections to Remote Internet Voting

Philipp Richter

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel
Wilhelmshöher Allee 64-66
34109 Kassel
Germany
prichter@uni-kassel.de

Abstract: Public voting in polling stations is believed to have a socioculturally-integrative effect, conveyed through the symbolic and ritualistic character of the election process. Remote internet voting is believed to not be able to provide this effect, because it omits the corporeal appearance at the polling station. The following contribution aims at indicating how such a sociocultural effect could be transferred from the real world polling station to remote internet elections.

1 The Public Nature of the Polling Station and Internet Elections

All forms of electronic voting, including internet voting, have been criticized for not fulfilling the Principle of the Public Nature of the Election which was declared as a constitutional principle in the Voting-Machine-Judgment of the German Federal Constitutional Court [BVerfG09] and which requires verifiability of the election for every citizen without special technical knowledge. Remote internet voting has additionally been accused of another shortcoming which the German legal literature has also located in the sphere of the Principle of the Public Nature of the Election. It has been brought forth that remote internet voting is not able to substitute the sociocultural integrative effect of public elections in real world polling stations, conveyed through the symbolic and ritualistic form of the election process. The corporeal act of voting at the polling station is described as the conscious exercise of a civil liberty as well as the perceptible expression of affiliation with the community to which is attested an identity-causing and ritualistic impact which politically integrates the voter and conveys to him a sense of the significance of the election [Ha04]. The "…polling station with its naked walls and shabby ballot boxes…" is described in contrast to the surroundings of the internet as a dramatization-free zone of political rationality [Me04]. The citizen is believed to experience himself through the ritual of the public election as sovereign and to gain the chance to identify with the state. This "symbolic-ritualistic character," which is attested to create a constituting effect in democratic elections, is believed to be "trivialized" and to dwindle in remote internet voting [Ka05]. Votes cast via the internet

are described as an unreflected act which is inadequate to the significance of an election and are even called “junkvote” [Bu01].
This criticism would mainly also be applicable to postal voting in which the corporeal appearance at the polling station is also omitted. In the Voting-Machine-Judgment this aspect of the public nature of elections was not addressed. The democratic-integrative effect of the election was based on the possibility for every citizen to fully monitor compliance with the election principles laid down in Article 38 of the German Constitution (GG). On the other hand, the Court was not called upon to say anything on this aspect, since the ruling only examined the use of on-site voting machines. It therefore remains unsettled, if a sociocultural effect as described is constitutionally required as part of the Principle of the Public Nature of the Election or if it is merely an effect caused by the established voting technique.
It shall not however be disputed here that such a symbolic-ritualistic effect of elections, aside from its dogmatic justification, is able to accomplish considerable integrative processes in democratic states. The abstract construct of the state becomes perceptible in symbols and rituals. By ritualistic participation of the citizens in matters which unite them and by establishing symbols for the display of common meaning, the community gains form, security and constancy [He83, p. 97]. Such symbols and rituals are widely known. The state, as a union of meaning and a body capable of acting, is perceptible in flags and emblems, in anthems, in the public meetings of parliaments and among many others also in the act of voting in public, in which moreover every eligible voter is able to take part actively. An election in a parliamentary democracy is the fundamental tool by means of which the citizens unite into a public body which is able to act. By active participation the citizens gain the possibility to take part in the installation of the organization called state and thus to perceive it as something of their own making, not as something ordered from above. Unity in meaning and unity in action by forming a public body are the two factors which in combination give the societal alliance its constancy [He83, p. 106 ff.]. In an election, they are exercised side-by-side and become perceptible by the symbolism and the ritual of the public act of voting.
It is however a misconception to believe that the described effect could only be conveyed by the corporeal act of voting in the real world, a misconception which oversees that the sociocultural effect of public voting could be conveyed in new ways by a medium like the internet [Ne02]. It has not been proved by which actions or symbols exactly the described effect is conveyed. Is it interaction and communication with other voters? Is it the reputable surrounding of the polling station? Is it the slowness of the process? Is it all of them together? Is it something else for each voter? The question would be very hard to answer.
However in the following, it shall be indicated how the central aspects of the act of voting in the real world polling station could be transferred to remote internet voting.

2 The Virtual Polling Station

Concepts for internet voting systems in respect to user interfaces up to now have usually aimed at offering a login and a digital ballot paper. Internet remote voting is therefore rightly sometimes called electronic postal voting [Ta99]. In this form, it uses only part of the potential of the IT-surroundings: the mobility of the voter in comparison with elections in polling stations, the speed of the transmission in comparison to postal voting, and the speed of the counting in comparison to both.
It does not, however, use the possibility to create virtual reality and thus to simulate the act of voting as a perceptible exercise. The polling station could be displayed graphically and entered by the voters via avatars.[1] Voters could enter the polling station simultaneously and thus interact as in the real world. This user interface could become the frame into which established internet voting concepts such as authentification, digital ballot paper, encryption, etc. could be embedded and which could extend them by the sociocultural effect of the public election. [2]

2.1 The Polling Station and the Voting Avatar

The polling station could be displayed as a three-dimensional graphical space. It could be designed following the model of a typical polling station in the real world, for example a school building. It could even imitate the real polling station for each electoral district. The virtual polling station thus could convey a reputable impression like real world polling stations are believed to do. Creating one virtual polling station for every polling station in the real world would mean higher expenses than creating only one virtual polling station for all absentee voters. It might however convey a high level of identification with the electoral district.
The voting avatar represents the voter graphically in the virtual world and allows him to move in the polling station and carry out the necessary steps of the election. It could look like the actual voter and thus make him visible to the other voters like in the real world polling station. If it would indeed be sensible to shape the avatar as the real voter, should be further discussed. At least the design of the avatar should stay within the scope of what is possible in the real world, so that it would be adequate to the significance of the election and not give the voting process the character of a game.

2.2 Chat

If one sees an important trigger for the sociocultural effect in interaction and communication with other voters, as possible in the real world polling station, this could be arranged in the virtual polling station by means of a general chat, a display by which text messages may be sent and read by all participants. Whoever would misemploy this application in order to disturb orderliness in the polling station, for example by polemic statements or molestation of other voters, could, exactly like in the real world, be expelled from the polling station, § 31 S. 2 *Bundeswahlgesetz* (BWG). The name of each voter or alias should be shown above the avatar so that chat messages can be linked to it.

---

[1] The use of 3D-surroundings and avatars in internet voting has also been proposed in order to attract younger people to internet voting in [MP04].

[2] Established concepts might also be extended at crucial points by the virtual polling station. Such aspects shall only be experimentally hinted at in this contribution, however.

2.3 Electoral Assistants

If one sees an important trigger for the sociocultural effect in communication with electoral assistants, who embody the state, even this could be arranged in the virtual polling station. Electoral assistants could also take part in the election process by means of avatars. By means of audio and video transmission as in VoIP-communication, they could even get in direct contact with voters and exercise classic duties of electoral assistants, for example identity controls and voting instructions. Maybe they might even monitor by video transmission that the secrecy of the vote is not broken by persons gazing at the voter's computer display. [3]
Internet voting is often seen as a way to make election assistants obsolete. This approach is however in conflict with the democratic ideal of a public citizen election, in which citizens take part on both sides of the ballot. It furthermore disregards the communicative potential of the internet. Also, a democratic monitoring of the election by citizens on both sides of the virtual ballot might be facilitated in this way.

2.4 Casting of Votes

The actual casting of the votes could be conducted classically by use of a digital ballot paper, which the voting avatar optically receives from the assistant avatar. The ballot paper could be filled out by the voter at a voting table and be dropped into the graphical ballot box. All IT-based concepts for the protection of the voting principles could and should be brought to bear in the vote casting. The virtual polling station cannot replace them. It would only convey the symbolic and ritualistic framework for the casting of votes.

2.5 Possible Election Procedure

The possible procedure of an election in the virtual polling station will now be outlined in order to make the specific chances and risks accessible to further analysis. Additionally the design of the virtual surroundings and their functional interaction can be described vividly in this way.
Every voter might be handed the necessary software and be assigned a temporary or permanent voting account, which would grant to him access to his avatar and to an instantiated[4] polling station. After logging in to his account, he might gain access to his avatar and might be given information on the voting procedure, the code of behavior in the polling station, and the possibilities for monitoring the election. He then might enter the virtual world with his avatar and appear, for example, on the street in front of the polling station.

[3] This idea would of course have to be designed as to be in compliance with the Privacy of the Home (Art. 13.1 GG) and the Informational Self-Determination (Art. 2. 1, Art 1. 1 GG).
[4] Instances in virtual worlds are closed areas, which may for example be entered only by certain users.

Here he might chat with other voters, exactly like in the real world. He might enter the polling station and, if one sees another trigger for the sociocultural effect of the election in the slowness of the procedure, get in line and wait for his turn. He might then approach an assistant avatar and interact with it. An audio-visual window might pop up by means of which voter and voting assistant might communicate directly. The voting assistant might brief the voter, check his identity, and eligibility. He might then hand over the digital ballot paper to the voter. This might be visualized by the assistant avatar handing a graphical ballot paper over to the voting avatar. The voter might walk his avatar over to a voting table and fill out the ballot paper. [5] During the act of casting the vote, nobody must be able to interfere with the voter or his avatar. The voter might then again interact with an assistant avatar or directly drop the graphical ballot paper into the ballot box. He then might leave the polling station and log out or, as in the real world, might chat with other voters on the street in front of the polling station.

2.6 Sociocultural Effect

The advocates of a symbolic-ritualistic effect, which can only be conveyed by the corporeal act of voting in the real world polling station, present triggers for this effect. These triggers are stimuli from the real world, like seeing other voters, the optical impression of the polling station, corporeal movement on the way to the polling station, etc. The described effect is a pattern-based reaction to these stimuli.
Stimuli from the real world may however be transferred into virtual worlds and the other way around [Fr05, para. 15 ff.]. By means of graphical simulation of procedures in real world polling stations, the stimuli of public voting may, to a large extent, be transferred into the process of remote internet voting and trigger correspondent pattern-based reactions in the voter.
During transfer, stimuli are subject to transformation processes. Transfers from one world to another, as would be the case here, are not complete [Fr05, para. 28 ff.]. Driving a car in the virtual world is only an abstraction of driving a car in the real world, different actions are necessary to succeed. This transformation is necessary to transfer a stimulus and the correspondent learned pattern from the real world into the natural laws of the virtual world [Fr05, para. 30 ff.]. In a successful transfer, the virtual world does not employ the same stimuli as in the real world, but an abstract version of the stimulus which is able to suggest a reaction pattern from the real world [Fr05, para. 32 ff.].
It is thus in principle possible to trigger the described sociocultural effect of public voting by a virtual version of the procedure in the real world polling station. How successful this transfer would be in respect to every single voter would depend on the quality of the stimuli which are used to simulate stimuli from the real world, which are believed to trigger the desired reaction pattern. These relations would have to be analyzed thoroughly.

[5] A graphical polling booth might also be installed. It would however fulfill no other function than the visual one and might lead the voter to the misconception that it would grant the secrecy of his digital vote.

Graphical depiction of the polling station, the voters, and of the vote casting however appear to be functional suggestions of the voting procedure in the real world with a relatively low effort of transfer. Direct audio-visual communication with election assistants would demand an especially low effort of transfer, namely that from an authentic live portrayal to a real person, a transfer exercised by humans for ages.
The virtual polling station might slow down the remote internet vote casting and remove from it the feeling of cursoriness. The voter would not switch back and forth between browser windows, between the election, commercials and videos, but his senses would be focused on the election process.
Experiences in virtual worlds, especially communication and interaction in three-dimensional graphical surroundings leave behind memories. Nobody who has ever exposed himself to this technology would dispute this. The possibility of stimulus transfers from real to virtual and the effectuality of virtual experiences for the real world has furthermore been widely proven and accepted in education and training. Pilots learn real aviation in simulators. Doctors exercise physiological training by means of computer simulations instead of test animals [Mü96] and train surgical operations on humans in virtual surroundings [MHB10].

2.7 Difficulties

The process of stimulus transfer and transformation from the real world polling station will only work, if stimuli from the real world are known. The reaction pattern of the public election can only be suggested by virtual stimuli, if people still exercise and thus learn the pattern in the real world. For people who know only the virtual polling station, different reactions might be triggered. In order to convey the same reaction to these possible future citizens, the patterns would either have to be trained in the real world or virtual stimuli would have to be found, which trigger the same reaction originally.
By graphically depicting the public election of the real world, the aspect of monitoring the election and the sociocultural effect of the election would no longer be made possible by the same means. When an avatar casts a vote, this act visualizes the election. The visualization however does not grant certainty of the successful vote cast. For verification other mechanisms would have to be applied, which would allow monitoring for everybody without special technical knowledge. Voters would have to be advised not to rely on graphic visualizations, which are not designed to convey trust, but symbolic and ritualistic effects.
Remote internet voting and especially the virtual polling station would demand a certain amount of skill in respect to computers and the internet as well as access to hardware and software. Since these are not given for all citizens, the described technology may not fully replace established voting techniques, but rather be an additional voting channel.
Virtual realities have up to now become commonly known mainly through entertainment, especially gaming. The concept of the virtual polling station might thus be attacked on the ground that it would further trivialize the act of voting and change it into a game. Such criticism would however oversee that technology, especially information technology, triggers specific effects only by its specific application [Ro93].The virtual polling station would have to be designed in a way that would be adequate to the fundamental significance of elections in parliamentary democracies and must not be designed following the aesthetics of entertainment.

3 Conclusion

By means of a virtual polling station as described above, remote internet voting could trigger the sociocultural effect of corporeal voting in the real world. Remote internet voting would not remain in the stage of electronic postal voting, but develop into an absentee election with virtual attendance. In comparison to postal voting, remote internet voting including a virtual polling station could thus considerably facilitate the sociocultural effect of absentee voting.

Bibliography

[Bu01] Buchstein, H.: Modernisierung der Demokratie durch e-Voting?, Leviathan 2/2001, p.147 (155).

[BverfG09] Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 123, p. 39.(68 ff.) http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html.

[Fr05] Fritz, J: Wie virtuelle Welten wirken, Bundeszentrale für politische Bildung, 2005, http://www1.bpb.de/themen/OI6VDV,2,0,Wie_virtuelle_Welten_wirken.html

[Ha04] Hanßmann, A.: Möglichkeiten und Grenzen von Internetwahlen, 2004, p. 185.

[He83] Heller, H.: Staatslehre, 6. Auflage, 1983.

[Ka05] Karpen, U.: Elektronische Wahlen?, 2005, p. 31.

[Me04] Meinel, F.: Öffentlichkeit als Verfassungsprinzip und die Möglichkeit von Onlinewahlen, KJ 2004, p. 414 (428).

[MHB10] Maschuw, K.; Hassan, I.; Bartsch, D.K.: Chirurgisches Training am Simulator, Der Chirurg 1 2010, p. 19.

[MP04] Maidou, A.; Polatoglou, H.M.: E-Voting and the architecture of virtual space, Electronic Voting in Europe –Technology, Law, Politics and Society, Workshop of the ESF TED Programme, 2004 in Bregenz, Lake of Constance, Austria, pp. 133. ff.

[Mü96] Müllges, K: Vom Brüllfrosch zur Computermaus, Deutsches Ärzteblatt 93, Heft 42, 18. Oktober 1996, p.69.

[Ne02] Neymanns, H.: Online-Wahlen, Buchstein/ Neymanns (Hrsg.), 2002, p. 36.

[Ro93] Roßnagel, A.: Rechtswissenschaftliche Technikfolgenforschung, 1993, pp. 72 f.

[Ta99] Tauss, J.: Die elektronische Briefwahl als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten, Jahrbuch Telekommunikation und Gesellschaft 1999, pp. 285 – 292.

Session 3: Certification and Evaluation of E-Voting Systems

A Formal IT-Security Model for the Correction and Abort Requirement of Electronic Voting[1]

Rüdiger Grimm[1], Katharina Hupf[1], and Melanie Volkamer[2]

[1]Institute of Information Systems Research
Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz
Germany
{grimm,hupfi}@uni-koblenz.de

[2]Center for Advanced Security Research Darmstadt
Technische Universität Darmstadt
Mornewegstraße 32
64293 Darmstadt
Germany
volkamer@cased.de

Abstract: This paper addresses a basic security requirement of electronic voting, namely that a voter can correct or abort his vote at any time prior to his final vote casting. This requirement serves as a protection against voter precipitance (haste). We specify rules for a reset and cancel function that implement the correction and abort requirement. These rules are integrated in an extended version of the formal IT security model provided in [VG08]. We show that these rules do respect the requirements covered in this model namely that each voter can cast a vote, that no voter loses his voting right without having cast a vote and that only eligible voters can cast a vote. This paper formally describes and mathematically proves the model and finally shows at which places of a voting process the formal rules apply.

[1] This paper is developed within the project "ModIWA – Modellierung von Internetwahlen" which is funded by DFG, and carried out at the Universities Kassel (Roßnagel, Richter) and Koblenz-Landau (Grimm, Hupf)

1 Introduction

Security is an elementary property of electronic voting systems and is thus fundamental for the trust of the voters in the system. Security objectives for electronic voting were first collected in an informal way, for example by a European-wide accepted recommendation adopted by the Council of Europe [CE04]. Later the semi-formal method of the Common Criteria [CC06] was used to specify a Protection Profile (PP) for a basic set of security requirements for online voting products [VV08]. There are good reasons to specify the security objectives of an IT system in a formal way, i.e., by mathematical calculus which states and proves properties clearly [Wa05]. The formalization of security objectives is a way to gain unambiguous and clearly understood

Requirements for electronic voting. Due to its formal base, it can be mathematically proven that a specification or implementation conforms to these formal security requirements. For example, the mandatory access model of Bell and LaPadula [BP73] strengthens the trust in a secure centrally controlled multi-user computer system, such that in the early days of computer system security evaluation it used to define the highest assurance level of the Orange Book Criteria [DD85]. Thus a formal IT security model on electronic voting defining security requirements from [CE04] and [VV08] in a formal language can create large amounts of trust in the effect of the security functions implemented in the electronic voting system.

However, the Common Criteria Protection Profile for online voting products [VV08] requires an evaluation according to evaluation assurance level EAL2+ on a scale from 1 to 7. This level does not require any formal proof. This evaluation level seems to be acceptable as this PP only claims to define basic requirements. Parliamentary elections, however, demand a higher evaluation level, probably EAL 6 or 7. At this level, the application of formal methods and the definition of a formal security model [CC06] are mandatory for the Common Criteria evaluation.

To enable a Common Criteria evaluation according to these levels, the authors of [VG08] provide an IT security sub-model for electronic voting. However, this model only covers a small subset of security objectives namely that each voter can cast a vote, that no voter loses his voting right without having cast a vote and that only eligible voters can cast a vote. This model needs to be extended to meet the remaining security objectives. The aim of this paper is to extend the protection against errors by haste (precipitation). Moreover, in extending the model in [VG08] we have found a weakness in the model which is corrected in this paper, as well.

Protection against errors by haste is a basic legal requirement well established in private and public law [Ba06]. This requirement is expressed by two security objectives in [VV08], “O.Correction” and “O.Abort,” as well as by the security objectives 10 and 11 in [CE04]. To meet these two security objectives, we will propose two functions “reset” and “cancel” of a voting process. The abortion of a voting process protects not only against precipitation, but it also protects the secrecy of voting against unwanted external events like the appearance of another person during the voting process. Thus reset and cancel are important for the support of the freedom of vote.

The paper is organized as follows: In the subsequent section 2 we quote those security objectives, from the Protection Profile on basic requirements for online voting products [VV08], that we are going to formalize in this paper. In section 3 we enhance the existing formal IT security model in [VG08] according to our findings and provide a full proof of its correctness. In section 4 we formalize the "reset" and "cancel" functions, which have been introduced in section 2. In section 5 we prove that this extended security model is correct and, thus, provides a smooth extension of the original security model [VG08]. To complete the picture, in section 6 we show (informally) at which points in a voting process our security rules of the formal model are applied. Finally, in section 7 we draw some conclusions from our work and point to further research.

2 Security Objectives

Security models start with the identification of security objectives [CC06, Gr08]. In the protection profile of a basic set of security requirements for online voting [VV08], a set of thirty-two security objectives for online voting products are specified. The following two of these have been used as a first step towards a formal model for remote electronic voting systems in [VG08][2]:

O.OneVoterOneVote: It is ensured that (a) each voter can cast one vote and (b) no voter loses his voting right without having cast a vote.

O.UnauthVoter: Only eligible voters who are unmistakably identified and authenticated are allowed to cast a vote that is stored in the ballot box.

These two objectives are met by specifying properties that define "secure system states" and rules to be applied on any function that securely transfers a system state into another system state. Therefore, these rules are called transition rules. After specifying the related security state properties and transition rules of these two security objectives, we will extend the model by including two more security objectives from [VV08], namely:

O.Abort: The voter can abort his voting process at any time prior to the final casting of the vote without loosing his right to vote.

O.Correction: There is no limit on the number of corrections a voter can make to his vote until the final casting of the vote.

These objectives will not be met by security properties, but by a further transition rule. We propose that "reset" and "cancel" functions are the appropriate prototype functions of this rule, whereby "cancel" will be a repetition of "reset" until the initial state of a voter's voting process. We will prove (in section 5) that these rules preserve the security properties of **O.OneVoterOneVote** and **O.UnauthVoter**.

[2] We refer to [VV08] as well. This paper formally models some basic security requirements for electronic voting, which apply to both voting machines and online voting.

The rules for allowed state transitions are to be implemented by voting products as functions for data processing. However, the rules do not determine appropriate places for these functions within a voting process. Strictly speaking, it is not the purpose of an IT security model to design processes or protocols. Although we are not going to design the voting process, we will show (in section 6) informally at which points in a voting process our rules (and especially the "reset" and "cancel" functions) would be applied.

3 The Basic Model

3.1 The original model of [VG08]

We quote the basic model from [VG08] in that we take the security objectives **O.OneVoterOneVote** and **O.UnauthVoter** and associate them with properties of a secure state and allowed state transitions. Before we define the security properties, we define (general) system states of a voting process:

Definition 1 (voting system state)

A system state $S := <W, V, voter>$ is represented by a triple of the following three entries:

1. W – Set of eligible voters (those who are listed in the electoral register and have not yet cast a vote).
2. V – Set of (encrypted) votes stored in the e-ballot box.
3. $voter: V \rightarrow M$ – Mapping of (encrypted) votes to their electors.

W_{total} is the set of all eligible voters registered by the responsible voting officials before the voting system is started. M is a superset of W_{total} that contains any user who tries to access the remote electronic voting system, whether or not this particular user has the right to cast a vote. The function *voter* assigns each (encrypted) vote to its producer (voter).

The initial state is defined as the triple $S_0 := < W_{total}, V_0=\{\}, voter_0=\{\}>$.

We assume that state transitions t_1, t_2 … that carry the system from state to state are stimulated by events such as the login of a voter into the system, the request of an empty voting ballot, the filling out of the ballot, the casting of a vote, etc.

$$S_0 \xrightarrow{t_1} S_1 \xrightarrow{t_2} \ldots \xrightarrow{t_i} S_i$$

Now we follow the basic model in [VG08] and proceed to defining secure system states, and then we state the rules for allowed state transitions.

Definition 2 (secure voting system state, basic version)

A state S_i is a secure state iff (all of) the following constraints hold:

OneVoterOneVote (*A*)	$\forall v, v' \in V_i : voter(v) = voter(v') \Rightarrow v = v'$
OneVoterOneVote (*B*)	$\forall w \in W_{total} \setminus W_i : \exists v \in V_i : voter(v) = w$
UnauthVoter	$\forall v \in V_i : voter(v) \in W_{total}$

Definition 3 (rules for permitted state transitions)

A state transition from state S_i to state S_{i+1} stimulated by event t_{i+1} is permitted, $permitted\left(S_i \xrightarrow{t_{i+1}} S_{i+1}\right)$, if one of the following rules holds:

[Rule 1] $W_i = W_{i+1} \wedge V_i = V_{i+1} \wedge voter_i = voter_{i+1}$

[Rule 2] $\exists v \in V_{i+1} : (voter_{i+1}(v) \in W_i \wedge W_{i+1} = W_i \setminus \{voter_{i+1}(v)\} \wedge V_i = V_{i+1} \setminus \{v\})$

[Rule 1] represents a state transition in which no vote is cast whereas [Rule 2] models a state transition during which an eligible voter casts a vote into the ballot box. This voter is eliminated from the list of eligible voters and his vote is stored in the ballot box.

3.2 Discussion of the original model

The security theorem in [VG08] proves that "for all permitted state transitions starting with the initial state [...] holds that any reachable state is secure." This security theorem is correctly proven. But it doesn't regard those secure states that are reached by an illegal state transition. Any state reachable by a permitted state transition from a secure state is obliged to be secure, even if the initial state (which is secure) has been reached for any reason by a non-permitted state transition. The following example shows that this isn't fulfilled for the formal security model in [VG08]:

Assume an eligible voter casts a vote into the ballot box, but –due to erroneous system implementation– the voter isn't eliminated from the list of eligible voters. The succeeding system state remains secure because *OneVoterOneVote(B)* doesn't specify properties of W_i, but only of $W_{total} \setminus W_i$. Suppose this voter casts a vote again. Since this voter is still eligible, his vote is stored in the ballot box and he is eliminated from the list of eligible voters. This represents a permitted state transition according to [Rule 2]. But the ballot box now contains two votes from the same voter. Thus an insecure system state is reached from a secure state by a permitted state transition.

To avoid this situation the definition of secure states needs to be extended such that a voter who has cast a vote into the ballot box is removed from the list of eligible voters. This can be incorporated into the formal model of [VG08] by extending definition 2 by an additional requirement for secure states:

$$OneVoterOneVote\ (C) \qquad \forall w \in W_i : \forall v \in V_i : voter(v) \neq w$$

Still, this extension isn't sufficient yet. Let S_i be a secure state. Furthermore, assume that an eligible voter x who hasn't yet cast a vote wants to vote. Let the system be in a state where the voter's eligibility is provable, i.e., $x \in W_i$. Due to an incomplete or incorrect list of registered voters, let $x \notin W_{total}$. This situation and $x \in W_i \setminus W_{total}$ are not forbidden by the definition of a secure state. Therefore, the system would follow [Rule 2] and let x cast a vote v, such that $V_{i+1} = V_i \cup \{v\}$ holds. Even though state S_i was secure and the state transition from S_i to S_{i+1} was permitted, state S_{i+1} isn't secure since $x = voter(v) \notin W_{total}$ violates the security property *UnauthVote*.

To avoid this situation, we add one more requirement for secure states, namely, that the system allows only registered voters ($x \in W_{total}$) to cast a vote ($x \in W_i$):

$$EligibleVoters \qquad W_i \subseteq W_{total}$$

This leads our enhanced security model's definition of a secure state.

3.3 The enhanced model

We now include the additional security properties *OneVoterOneVote* (*C*) and *EligibleVoters* from our discussion in section 3.2 above to the three security properties *OneVoterOneVote* (*A* and *B*) and *UnauthVoter* from definition 2 in section 3.1 above and thus we get the final definition of a secure state by these five security properties:

Definition 4 (secure voting system state, advanced version)

A voting system state S_i is a secure state if (all of) the following constraints hold:

$OneVoterOneVote\ (A)$	$\forall v, v' \in V_i : voter(v) = voter(v') \Rightarrow v = v'$
$OneVoterOneVote\ (B)$	$\forall w \in W_{total} \setminus W_i : \exists v \in V_i : voter(v) = w$
$OneVoterOneVote\ (C)$	$\forall w \in W_i : \forall v \in V_i : voter(v) \neq w$
$EligibleVoters$	$W_i \subseteq W_{total}$
$UnauthVoter$	$\forall v \in V_i : voter(v) \in W_{total}$

Obviously, the five properties above are equivalent to the two following properties:

(ap.1) *voter* is an injective function (equivalent to *OneVoterOneVote* (*A*)),

(ap.2) $W_{total}=W_i+voter(V_i)$ ("direct sum", equivalent to the other four properties). The direct sum means that both hold, $W_i \cup voter(V_i)=W_{total}$, and $W_i \cap voter(V_i)=\varnothing$.

The proof that (ap.1) and (ap.2) are equivalent to definition 4 is straight forward and left as an exercise to the reader. It is also easy to see that the initial state S_0 is secure, because the voter function is empty, and hence injective; and $W_0 \cup voter(V_0)=W_{total} \cup \varnothing=W_{total}$ *; and* $W_0 \cap voter(V_0)= W_{total} \cap \varnothing=\varnothing$.

Security Theorem

Permitted state transitions of definition 3 carry secure states into secure states according to definition 4.

Proof: In [VG08] we proved the security theorem in the weaker version that starting with S_0 any sequence of allowed state transitions would always lead to a secure state. We had to prove this by mathematical induction. Here we prove a stronger version that starting from any secure state (regardless of how this state was reached) an allowed state transition according to [Rule 1] or [Rule 2] will always reach a secure state. That is, we have to prove directly: For any $i \geq 0$, if we assume that S_i is secure, i.e., it has properties (ap.1) and (ap.2), and that $permitted\left(S_i \xrightarrow{t_{i+1}} S_{i+1}\right)$, i.e., t_{i+1} follows [Rule 1] or [Rule 2], then we have to show that properties (ap.1) and (ap.2) also hold for S_{i+1}.

Let t_{i+1} follow [Rule 1]. Then $V_{i+1}= V_i$ and $W_{i+1}= W_i$ and $voter_{i+1}= voter_i$, thus S_{i+1} simply inherits the security properties (ap.1) and (ap.2) from S_i.

Let t_{i+1} follow [Rule 2]. Then exactly one eligible voter casts a vote v into the ballot box during state transition t_{i+1}. Thus, $W_{i+1}= W_i \setminus \{voter_{i+1}(v)\}$ and $V_{i+1}= V_i \cup \{v\}$ holds.

(ap.1) Then $voter_{i+1}$ is injective on $V_i \cup \{v\}$, because $voter_{i+1}$ restricted on V_i is, by definition, equal to $voter_i$, which is injective, and $voter_{i+1}(v)$ does not match with any other image of $voter_i$, because $voter_{i+1}(v) \in W_i \setminus W_{i+1} \subset W_i$ and hence cannot have been in $voter_i(V_i)$ since $W_i \cap voter(V_i) = \emptyset$.

(ap.2) *(i)* $W_{i+1} \cup voter(V_{i+1}) = (W_i \setminus \{voter(v)\}) \cup voter(V_i \cup \{v\}) = (W_i \setminus \{voter(v)\}) \cup (voter(V_i) \cup \{\text{voter}(v)\}) = W_i \cup voter(V_i) = W_{total}$. The last equality holds because S_i has property (ap.2).

(ii) $W_{i+1} \cap voter(V_{i+1}) = (W_i \setminus \{voter(v)\}) \cap voter(V_i \cup \{v\}) = (W_i \setminus \{voter(v)\}) \cap (voter(V_i) \cup \{\text{voter}(v)\}) = W_i \cap voter(V_i) = \emptyset$. The last equality holds because S_i has property (ap.2).

4 An additional transition rule for "reset" and "cancel"

In this section we incorporate the security objectives *O.Abort* and *O.Correction* into the enhanced formal model. For this purpose we introduce an additional transition rule [Rule 3], which meets these objectives and will, therefore, be associated with a secure "reset" and "cancel" function.

4.1 Informal description of "reset" and "cancel"

While *O.Abort* is correlated with the sending and receiving of "cancel," *O.Correction* is associated with the sending and receiving of "reset." With "reset" we mean that during a voting process a voter can go back one step just before the last message that he sent to the server. With "cancel" we mean, that a voter can repeat reset events back to the initial state so that he can restart his individual voting process. On the receiving side, after a voter's "reset" the voting server must filter out all events that were stimulated by messages exchanged with this voter just before the last message received from this voter. However, all other events stimulated by messages with other voters must be kept by the voting server. On receiving a "cancel" message from a voter, the voting server must forget all events by messages exchanged with this voter, but keep all events stimulated by other voters. The sending and receiving of a "reset" and "cancel" message must be carefully synchronized between voters and their voting server. As a security rule, the "reset" must not create or delete voting rights or cast votes

4.2 Formal basics

The formalization of the "reset" and "cancel" functions requires some formal basics on lists and list operations and a communication function on events. Readers who are familiar with the formal specifications can skip to section 4.3.

Let M denote the set of all communication partners. Then we assume communication partners a, b, $\ldots \in M$ who observe events that are correlated by a communication function *com*. Partner a will be a model for a voter and partner b will be a model for a voting server. Each partner observes events on his side that are stimulated by the sending and receiving of messages. Events are communicated via messages. If a sends a message of type e to b, then a observes the event of type e that he sends to b, and b would observe this event with the label e as a message of type e that he receives from a. In the following we will use the terms "message" and "message type" with the same meaning as "event" and "event label", respectively. We will sometimes say, "sending event" and "receiving event" instead of "sent message" or "received message." The following event labels (=message types) are useful for the modeling of electronic voting, e.g., [VV08]. Note that they are just an example which we will take up in section 6. They are not exhaustive. For example, message types "error" or "verify" are ignored throughout this paper's model.

$$Eventlabels = \{\pm login, \pm requestBallot, \pm vote, \pm reset, \pm cancel, \pm confirmBallot, \pm castVote, \pm feedback, \pm logout\}$$

Let $e \in Eventlabels$ then $sig(e)$ denotes the algebraic sign of e. A negative sign of an event label e indicates that the associated event is being sent, e.g., $e = -login$. A positive sign indicates the associated event is being received, for example, $e = confirmBallot$.

Events are event labels associated with their sender and recipient. We denote the set of all possible events as

$$Events \subseteq Eventlabels \times M \times M$$

Let $a,b \in M$ and $e \in Eventlabels$. Events are defined as triples, but for convenience we will use the following notation for events instead (cf. [Gr09]):

$a(e:b)$	a receives a message e from b
$a(-e:b)$	a sends a message e to b

Let for $1 \leq k \leq n$ π_k denote the set-theoretic projection of a Cartesian product of n sets on its k-th component. Let $x = a(\pm e:b)$ be an event and π_i the projection of a tuple to its i-th element, then

$\pi_1(x)$ returns the event label e of x, which may carry a positive or negative sign.

$\pi_2(x)$ returns $a \in M$. Note that a is the sender of the message e if $sig(e)$ is positive, and a is the recipient if $sig(e)$ is negative.

$\pi_3(x)$ returns $b \in M$. Note that b is the recipient of the message e if $sig(e)$ is positive, and b is the sender if $sig(e)$ is negative.

For the synchronization of events that are stimulated by messages between a and b, we need a way to express that a message is observed by both sides. Let *Events* be the set of all possible events, $a,b \in M$ and $e \in Eventlabels$. The function *com* is defined as in [Gr09] and maps the sending and receiving of a message on the corresponding event on the partner's side:

com: $Events \rightarrow Events$

$com(a(e{:}b)) := b(-e{:}a)$

$com(a(-e{:}b)) := b(e{:}a)$

We are going to collect events in ordered lists of events which allow us to operate on sequences of events and on identified events within the list. The algebra of ordered lists is a standard formalism used in theoretical computer science, see for example [MG08]. As usual, a list of events is understood as a finite sequence (or n-tupel) of these events. If *op* is a function on lists, for example the deletion of its head element, then the k-times repetition of the operation is denoted as $op^k(L) = op_k(op_{k-1}(...(op_1(L))...))$.

Useful list functions are [MG08]:

- For any list L of elements of a set Q, $set(L) \subset Q$ denotes the (unordered) set that consists of all elements of L.
- *head(L)* and *tail(L)* return the last element of L, and the rest of the list L without the last element, respectively. In contrast, $\overline{tail}$ is complementary to *tail* and returns the remaining list without the first element of L.
- Let $q \in Q$, then $L||q$ appends the element q at the end of the list L.
- $|L|$ returns the number of elements in L.
- Assume $n \in \mathbb{N}$ a natural number and $q \in Q$. $L[n]$ returns the element at the n-th position in the list and $pos(L,q)$ returns the position of the last occurrence of the element q in the list L.
- $del(L,l)$ with $l \in \mathbb{N}$ a natural number returns the list L, from that the l-th and all succeeding elements are removed.
- Especially for lists L of events, we define a filter function, a remove function and a select function. For an event x and $k \in \{1,2,3\}$, $filter_k(L,x)$ removes all events with event label x from the list L if k=1, or it removes all events whose first or second actor is x from the list L if k=2,3, and then returns the remaining list. For a communication partner a, $rmv(L,a)$ returns the list L from which all events that were sent *or* received by a are removed. The function $select_k(L,x)$ returns the list of events where only those events with the event label x are contained if k=1, or only those events whose first or second actor is x are contained if k=2,3.

4.3 Formalized “reset” and “cancel”

We are now ready to formally define the “reset” and “cancel” event and prove the important synchronization theorem. For simplicity we assume in the following that a communicates solely with b, while b communicates with a and other partners as well. Thus in the model, a represents a voting client and b represents the voting server.

Definition 5 (Reset)

Let $a,b \in M$ and X_i be the list of events on the side of communication partner a , i.e., $\forall x \in X_i : \pi_2(x) = a$. Furthermore, let Y_j denote the list of events on the side of communication partner b. Let *sent(X_i)* denote the list of events that contains the send-events of X_i only, and let *received(Y_j)* denote the list of events that contains the receive-events of Y_j only, then we define:

$$X_i \parallel a(-reset : b) := \begin{cases} X_0 & if \quad set(sent(X_i)) = \emptyset \\ del(X_i, l) & else, where \quad l = \max\{ n \in N \mid x_n \in set(sent(X_i)) \} \end{cases}$$

$$Y_j \parallel b(reset : a) := \begin{cases} del(Y_j, k) \parallel rmv(\overline{tail}^k(Y_j, a)) & if \quad C_2 \\ filter_3(Y_j, a) & else \end{cases}$$

where C_2 is $\exists k > 0 : k = \max\{n \in N \mid y_n \in set(received(filter_3(Y_j, a)))\}$

Explanation: If a communication partner $a \in M$ executes a “reset” then the last event $x_l \in X_i$ which is sent by a and all successive events to x_l are deleted. If there is no event in X_i that is sent by a (i.e., X_i is empty or contains only received events), then X_i is set to its initial state.

If a communication partner $b \in M$ receives a “reset” then the last event $y_k \in Y_j$ that is received by b from a is deleted as well as all successive events to y_k, which are sent to or received from a by b. Remark that all events successive to y_k, which are exchanged with other communication partners, are preserved in the state of communication partner b. If there is no event in Y_j that is received from a by b (i.e., Y_j is empty, doesn't contain any events exchanged with a or contains only events sent to a), then all messages sent by b to a are deleted from the list Y_j, i.e., b is set to initial state with respect to a. All events that are exchanged with different communication partners are preserved.

General Assumptions:

The reset and cancel functions are to be synchronized between voters and server. They wouldn't work properly if the system is interrupted. Therefore, availability is a security requirement for all communication functions. For the purpose of our security considerations, we assume that our systems are available and work correctly. Therefore, we assume secure communication channels in the following sense:

(A1) $\exists i \geq 0 : x \in set(X_i) \quad \Leftrightarrow \quad \exists j \geq 0 : com(x) \in set(Y_j)$

If a communication partner *a* exchanges a message *x* with *b* then there exists a state such that this message is observable on the partner's side.

(A2) $\forall i > 0 : \forall x_n, x_m \in set(sent(X_i)) : pos(X_i, x_n) < pos(X_i, x_m) \quad \Leftrightarrow$
$\forall j \geq i : pos(Y_j, com(x_n)) < pos(Y_j, com(x_m))$

If a communication partner *a* sends two messages in a particular order then the communication partner *b* receives them in exactly that order.

Theorem (Synchronization property of "reset")

In a secure communication environment (i.e., A1, and A2 hold) the sending and receiving of "reset" events are well synchronized. Formally: $com(head(sent(X_i \,||a(\text{-}reset{:}b)))) = head(received(select_3(Y_j||\, b(reset{:}a),a)))$.

Proof:

Given the two assumptions (A1) and (A2). Furthermore, we denote C_1: $set(sent(X_i)) \neq \varnothing$, i.e., *a* hasn't sent anything so far and C_2: $set(received(filter_3(Y_j,a))) \neq \varnothing$, i.e., *b* hasn't received any message from *a*. According to definition 5 of "reset," the following four possibilities exist:

1. *Neither C_1 nor C_2 holds.*

   Then $X_i \,||a(\text{-}reset{:}b) = \varnothing$ and $select_3(Y_j||b(reset{:}a)) = select_3(filter_3(Y_j,a)) = \varnothing$. Obviously, Theorem 1 is true.

2. *C_1 does not hold, but C_2 holds.*

   This directly contradicts assumption (A1). If there was no message sent by communication partner *a*, then there can't be any message received from *a* by *b*.

3. *C_1 hold and C_2 does not hold.*

   This is a direct contradiction to assumption (A1) as well. If there was no message received by *b* from *a*, then there can't be any message sent from *a* to *b*.

4. *C_1 and C_2 hold.*

Let x_l be the last event sent by *a* before executing reset. Due to premise (A2), $head(received(select_3(Y_j,a))) = com(x_l)$ holds. On the side of communication partner *a*, the event x_l and all successive events to x_l are eliminated during the execution of reset. On the side of communication partner *b*, the event $com(x_l)$ and all successive events to $com(x_l)$ that are exchanged with the communication partner *a* are eliminated during the execution of reset. All events successive to event x_l that are exchanged with different communication partners are preserved.

If $set(sent(X_i \,||a(\text{-}reset{:}b))) = \varnothing$ holds, then due to premise (A1) $set(received(select_3(Y_j \,|| \, b(reset{:}a),a))) = \varnothing$ holds as well. Thus Theorem 1 holds.

Assume $sent(X_i \,||a(\text{-}reset{:}b)) \neq \varnothing$ and *let* $x_m = head(sent(X_i \,||a(\text{-}reset{:}b))$ be the last sent event after the execution of "reset." Given precondition (A1) there exists a state on the partner's side such that $com(x_m) \in Y_j \,||\, b(reset{:}a)$. Furthermore, in accordance to premise (A2) $com(head(sent(X_i||a(\text{-}reset{:}b))) = head(received(select_3(Y_j||b(reset{:}a),a)))$ holds.

Definition 6 ("Cancel")

Let $a,b \in M$ and X_i be the list of events on the side of communication partner a, i.e., $\forall x \in X_i : \pi_2(x) = a$. And let Y_j be the list of events on the side of communication partner b, respectively. Then we define:

$$X_i \parallel a(-cancel : b) \quad := \quad X_0$$

$$Y_j \parallel b(cancel : a) \quad := \quad filter_3(Y_j, a)$$

Explanation: If a communication partner a executes a "cancel", then he is set back to his initial state with an empty event list X_0. If a communication partner b receives a "cancel" from communication partner a, then all events sent to or received from a by b are eliminated from his event list.

Remark:

According to definition 6 the following holds: Let $k := |sent(X_i)|+1$ be one more than the number of all sending events in the list of events on the side of a, and let $l := |received(filter(Y_j,a))|+1$ be one more than all events that b has received from a, then

$$X_i \parallel a(-cancel : b) \quad = \quad X_i \parallel^k a(-reset : b) \quad = \quad X_0$$

$$Y_j \parallel b(cancel : a) \quad = \quad Y_j \parallel^l b(reset : a) \quad = \quad filter_3(Y_j, a)$$

The execution of "cancel" by a communication partner a can be expressed by means of the event "reset". Communication partner a executes $a(-reset:b)$ for each event sent by him, until there are no events left or only events that are received by a. By executing an additional $a(-reset:b)$, a is set to its initial state with empty event list X_0.

The execution of "cancel" on the partner's side can be specified by the means of the event "reset" as well. Communication partner b receives $b(reset:a)$ for each event received from a. The remaining events are all either sent from b to a or are messages exchanged with other communication partners different than a. The remaining events sent to a are deleted by the execution of an additional $b(reset:a)$.

In the next step we must make sure that "reset" cannot produce insecure states, i.e., we have to specify a transition rule for "reset".

4.4 Transition rule for "reset"

A state transition from state S_i to state S_{i+1} stimulated by event t_{i+1}=a(–reset:b) is permitted, $permitted\left(S_i \xrightarrow{t_{i+1}} S_{i+1}\right)$, if the following rule holds:

[Rule 3] Let T_i be the list of events observed by a before the execution of "reset," and let T_{i+1} be the list of events observed by a after the execution of reset, and let $l := |T_{i+1}|$ be the length of list T_{i+1}. Furthermore, let $T := \overline{tail}^{l}(T_i)$ be the list of reverted events. Then t_{i+1}=a(–reset:b) is permitted iff

$$(a \in W_i \cap W_{i+1}) \wedge (\forall 1 \leq j \leq |T|: \; permitted\left(S_{l+j} \xrightarrow{T[j]} S_{l+j+1}\right))$$

Explanation: According to [Rule 3], a state transition from state S_i to state S_{i+1} stimulated by event $t_{i+1} = a(\text{-}reset\text{:}b)$ is an allowed state transition if the voter is eligible and has not yet cast his vote, both, before and after, the execution of "reset" ($a \in W_i \cap W_{i+1}$) and all reverted state transitions were permitted ($permitted\left(S_{l+j-1} \xrightarrow{T[j]} S_{l+j}\right)$).

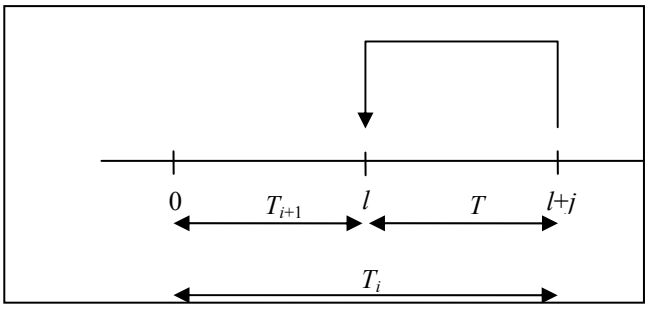


Figure 4.1: Relation between the list of events before and after the execution of "reset."

Remark: [Rule 3] is compatible with both rules, [Rule 1] and [Rule 2], because it resets only permitted transitions. [Rule 3] conforms to [Rule 1] because by the reverted state transitions no vote had been cast into the ballot box. [Rule 3] is compatible with [Rule 2] because the resetting voter would not be one of those voters who had cast votes into the ballot box. Due to the definition of the "reset" function (the filter function in definition 5 makes sure that actions of other participants remain untouched!), the ballots of the other voters would not be reverted, of course.

5 The extended model

In this section, we show that [Rule 3] complies with the security properties (ap.1) and (ap.2) which are equivalent to definition 4.

The specification of an IT security model requires first the specification of secure system states and of permitted state transitions [Gr08]. As a definition for secure system states, we use the definition 4 of section 3.3 above in the version with the two properties (ap.1) and (ap.2), namely that *"voter* is an injective function" (ap.1) and that "W_{total}=W_i+*voter*(V_i)" (ap.2).

Extended security theorem

Permitted state transitions according to [Rule 1] and [Rule 2] of definition 3 as well as according to [Rule 3] from section 4 carry secure states into secure states according to definition 4. Formally, if a state S_i is secure and $permitted\left(S_i \xrightarrow{t_{i+1}} S_{i+1}\right)$, then S_{i+1} is also a secure state.

Proof of the security theorem: For [Rule 1] and [Rule 2] we have proven the security theorem already in section 3. We have only to prove the security theorem with respect to [Rule 3] of secure "resets." To simplify the proof, we first prove the following lemma:

Lemma 1: If a state S_i is secure and $permitted\left(S_{i-1} \xrightarrow{t_i} S_i\right)$, then S_{i-1} was a secure state.

Proof of Lemma 1: If S_i is a secure state and t_i was a permitted state transition, then the state transition t_i was performed according to [Rule 1] or by [Rule2]:

[Rule 1]: Then $V_i = V_{i-1}$ and $W_i = W_{i-1}$ hold. Since S_i is secure, S_{i-1} was secure as well.

[Rule 2]: Then there exists exactly one vote v" that has been put into the ballot box during state transition t_i such that $V_{i-1} = V_i \setminus \{v"\}$ and $W_{i-1} = W_i \cup \{voter(v")\}$. It has to be proven that the properties (ap.1) and (ap.2) hold for S_{i-1}.

(ap.1) Firstly, *voter* is injective on V_{i-1} because $V_{i-1} = V_i \setminus \{v"\} \subset V_i$, and *voter* is assumed to be injective on the full V_i already.

(ap.2) Secondly, it must be shown that $W_{i-1}+voter(V_{i-1})=W_{total}$:

(i) $W_{i-1} \cup voter(V_{i-1}) = W_{total}$ holds because *voter* is injective, and therefore $W_{i-1} \cup voter(V_{i-1}) = W_i \cup \{voter(v")\} \cup voter(V_i \setminus \{v"\}) = W_i \cup \{voter(v")\} \cup (voter(V_i) \setminus \{voter(v")\}) = W_i \cup voter(V_i) = W_{total}$. The last equality holds because *Si* is assumed to be secure.

(ii) $W_{i-1} \cap voter(V_{i-1}) = \emptyset$ is true because:
$W_{i-1} \cap voter(V_{i-1}) = (W_i \cup \{voter(v'')\}) \cap voter(V_i \setminus \{v''\})$. Since S_i is a secure state such that $W_i \cap voter(V_i) = \emptyset$ holds, it is sufficient to prove that $\{voter(v'')\} \cap voter(V_i \setminus \{v''\}) = \emptyset$ holds. And this is true because *voter* is injective.

This completes the proof of Lemma 1.

Given the Lemma 1 above, the proof of the security theorem with respect to [Rule 3] is trivial: If t_{i+1} follows [Rule 3] and S_i was secure, then all reverted state transitions were permitted according to [Rule 3], and hence S_{i+1} is a secure state according to our Lemma 1 above. □

6 Transition rules in a voting process

In the previous sections we have specified conditions for allowed state transitions. In this section we show, at which points in a voting process these rules are to be applied. There are several variants conceivable for each voter's polling process [VV08]. Since we are not going to discuss process designs, we have chosen one process variant with login at start of the voting process.

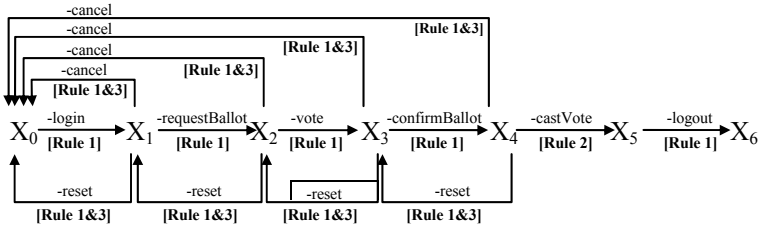


Figure 6.1: Mapping of transition rules on a (simple version of a) voting process

A sequence of transitions of the polling process is exemplarily shown in figure 6.1 where only the client side of the electronic voting process is considered. The voter identifies and authenticates himself by sending his data to the voting server (*-login*). If the voter is unmistakably identified and authenticated on the server's side, the voter is able to request the ballot form (*-requestBallot*). The ballot form is displayed on the voter's client and the voter makes his voting decision (*-vote*). The voter has to confirm his ballot (*-confirmBallot*) to protect against errors by haste. Afterwards he casts a vote into the ballot box (*-castVote*), where the casting of the vote follows [Rule 2]. The voter is allowed to correct his vote (*-reset*) or abort (*-cancel*) his voting process any time prior to the final casting of the vote, where "reset" and "cancel" follow [Rule 1] and [Rule 3].

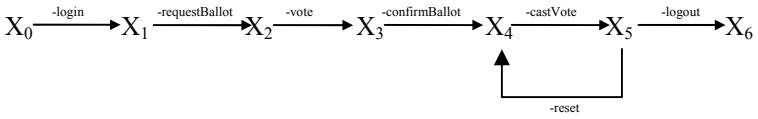


Figure 6.2: Example of an illegal placing of "reset" in the voting process

But the voter should not be allowed to correct or abort his vote after the final casting of his vote, as shown in figure 6.2. If he could do that, he would obtain the possibility to cast a vote into the ballot box for a second time. Note that our recommendation for the placement of "reset" and "cancel" complies with the security transition [Rule 3] which states that the voter is eligible, both, before and after the execution of "reset" and that all reverted state transitions were permitted.

7 Conclusion

In this paper an IT security model formalizes some basic security requirements for electronic voting: one voter one vote, eligible voters, the correction of a vote, and the abortion of a voting process. The corresponding security properties are specified as secure system states. The voting functions are controlled by state transition rules. We prove mathematically that a function following the rules would transfer a secure state into a secure state.

This contribution demonstrates how security requirements for electronic voting can be formalized and how an existing IT security model can be extended by adding gradually security objectives. However, we have not yet included anonymity or verifiability in our model. For a complete formalization of the security requirements for electronic voting, the IT security model presented in this paper needs to be extended by the remaining security objectives defined in the Protection Profile [VV08] and [GH09] step-by-step. Our next research step is to incorporate voter anonymity.

Bibliography

[Ba06] Bachmann, Gregor: Private Ordnung („Private Regime“). Jus Privatum 112, Mohr Siebeck, Tübingen 2006. Esp. S. 293 on precipitance and legal certainty of promises, also in the Anglo-Saxon legal domain.

[BP73] D. E. Bell and L. J. LaPadula. Secure Computer Systems: Mathematical Foundations, and A mathematical model. ESD-TR-73-278, MTR-2547, Vols 1&2. The MITRE Corporation, Bedford, MA, Nov 1973.

[CC06] Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, Version 3.1, 2006

[CE04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation rec(2004)11 adopted by the committee of ministers of the Council of Europe and explanatory memorandum. Strassburg, 2004.

[DD85] US Department of Defense: Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Dec l985, http://csrc.nist.gov/publications/history/dod85.pdf [25 Feb 2010]

[GH09] Grimm, R., Hupf, K.: Sicherheitsanforderungen an Onlinewahlen, In: Pichler (Hrsg.), Österreichischer Workshop über Elektronische Wahlen, Salzburg, Dezember 2009.

[Gr08] Grimm, R.: IT-Sicherheitsmodelle. Technical Report 03/2008, Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau, 2008

[Gr09] Grimm, R.: A Formal IT-Security Model for a Weak Fair-Exchange Cooperation with Non-Repudiation Proofs. In SECURWARE 2009, The Third International Conference on Emerging Security Information, Systems and Technologies, Athens, 18-23 June 2009. IEEE Computer Society Press, 2009

[MG08] MIT/GNU Scheme 7.7.90+, Chap. 7 Lists, MIT, Boston Massachusetts, 2008, http://www.gnu.org/software/mit-scheme/documentation/mit-scheme-ref/ [25 Feb 2010]

[VG08] Volkamer, M., Grimm, R.: Development of a Formal IT Security Model for Remote Electronic Voting Systems. In Electronic Voting, pages 185-196, 2008.

[VV08] Volkamer, M., Vogt, R.: Common Criteria Protection Profile For Basic Set of Security Requirements for Online Voting Products. BSI-CC-PP-0037, Version 1.0, 18. April 2008. http://www.bsi.bund.de/ [visited Feb 8, 2010]

[Wa05] Wang, Andy Ju An: Information Security Models and Metrics. Proceedings of the 43rd ACM Southeast Regional Conference, Vol 2, Security Session, 2005, pp. 178 - 184.

Compliance of POLYAS with the Common Criteria Protection Profile - A 2010 Outlook on Certified Remote Electronic Voting

Niels Menke and Kai Reinhard

Micromata GmbH
Marie-Calm-Str. 1-5
34131 Kassel
Germany
n.menke@micromata.de, www.polyas.de

Abstract: In 2008, the German Federal Office for Information Security issued the common criteria protection profile for Online Voting Products (PP-0037). Accordingly, we evaluated the Polyas electronic voting system, which is used for legally binding elections in several international organizations (German *Gesellschaft for Informatik*, GI, among others), for compliance with the common criteria protection profile and worked toward fulfilling the given requirements. In this article we present the findings of the process of creating a compliant security target, necessary restrictions and assumptions to the system design as well as the workings of the committee, and architectural and procedural changes made necessary.

1 Introduction

The remote electronic voting system Polyas has been in use since 1996 in international remote electronic voting projects like the elections of the German Society for Informatics (GI), the *Deutsche Forschungsgesellschaft* (DFG), Swiss Life Group Elections, and Finnish as well as German youth elections [RJ07]. As of 2010, about a million legally binding votes have been cast using the Polyas system, supporting different methods of authentication as well as rigorous documentation while maintaining a high level of anonymity and integrity.

In 2008, the German Federal Office for Information Security and its advisory board released and certified the common criteria protection profile for remote electronic voting systems [PP08]. Since then, it has been the ambition of Polyas' developers to certify the compliance of its system and architecture with the common criteria. Toward this goal we completed a security target for the existing Polyas system based on the protection profile and adjusted the system as well as defining restrictions where necessary.

In this paper we will present the workings of Polyas and the changes made necessary to achieve compliance with the requirements of the common criteria at large and the protection profile in particular, thereby showing possible solutions to typical problems when building electronic voting systems to be evaluated against the existing common criteria protection profile.

2 The Polyas voting process, revised

2.1 Overview

Polyas, among the electronic voting systems available on the market, is classified as a remote electronic voting system aka Internet voting system [VK06].
The most common variant of Polyas, which is to be discussed in this paper, uses a secret-based authentication by a common username/password process (see also [PP08] p. 16f.). While other variants of voter-authentication, namely, OpenID or Smartcard, exist and can be deployed on top of the core system, they are considered experimental at this point of time and therefore not yet to be evaluated against the common criteria protection profile.
Polyas ensures anonymity in the voting phase by means of a separation of duty among its components (see also [RJ07]). Voting with Polyas takes place by means of a Web browser (thin-client). While rich-client architecture is also available and can be used on demand of the voting committee, it is not yet subjected to common criteria evaluation.

2.2 Polyas general architecture—Achieving a separation of duty

The general concept of Polyas' architecture is inspired by real world ballot box voting sites (see figure 1). An electoral registry holds the authentication details and provides the point of entry for the voter who is going to cast his vote. The voter will hand his authentication credentials to the registry server, which will verify these credentials.
To ensure that the registry has not been compromised, the credentials are signed with a validation signature that resides on a third, separate validation server, and will be verified in case of authentication. Following a Two-Man-Rule, both the validation server and the electoral register will need to approve the credentials' authenticity before the voter will be issued a temporary voting token, and, with it, the opportunity to cast his vote.
To ensure that the same credentials are not used more than once for different voters (or voters unknown at the time of signing) the validator stores the signature after the first successful authentication attempt and together with the electoral register, will reject any credentials that are not eligible to cast a vote (see figure 2).

Once the voter has received his voting token, he is passed to the ballot box server, which presents one or more virtual ballot papers for the voter to cast his vote. Once the voter has successfully cast his vote, the temporary voting token is deleted from the system, thereby destroying any link between the voter's identity and his then-cast vote.

The election process from pre-voting phase to post-voting phase is to be electronically managed and overseen by the voting committee by means of a separate system. This system will, for example, allow the committee to monitor how many votes have been cast, how many voters have been marked as having voted, oversee the system health and functionality of the other components as well as starting, stopping, and finally counting the entire vote once a configurable number of committee members has authorized each of these respective processes.

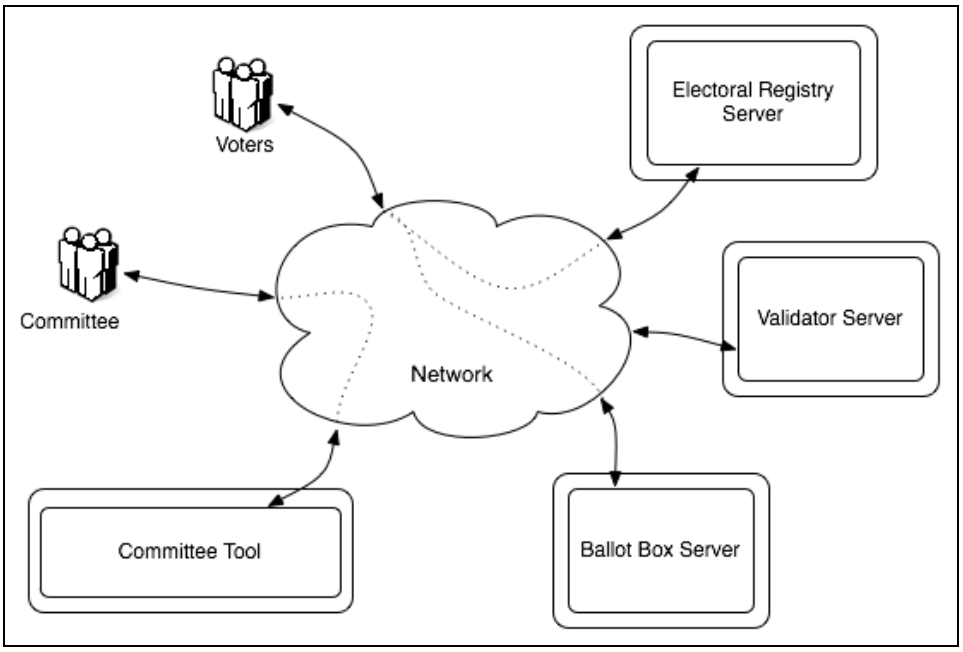


Figure 1: Polyas Architecture

2.3 Process Overview

Pre-Voting There are six steps that need to be undertaken before an election can be started (See also [RJ07]):

- Installing the Polyas software on each individual server. The software should be signed to recognize software manipulation in the post-voting process.
- Generating the authentication credentials, signing them with the validators' signature, and storing them in the registry.
- Sending the authentication credentials to each respective voter. Credentials will be sent under cover and need to be revealed (a one-way-process) by the voter in order to view it.

- For each of the four Polyas components, an https, a communication, and a database key pair must be generated. The https public keys will be shared. The private communication and database keys shall be encrypted, and one pass phrase for each of the keys must be entered. These pass phrases may form an additional layer of separation of duty for the vote-starting process as they can be handed out to different members of the committee and entered separately into the committee-tool.
- The private communication keys of the ERS and VS are used to sign the hashed credentials of each respective voter. Let sk_{VS} be the validators' communication key and sk_{ERS} be the electoral registry's communication key.
  Further, let *hash* be the SHA-256 hashing function and *sig* be the RSA signature function.
  Then each column will contain:

  $$ID - hash(Pw) - sig_{ERS} - sig_{VS}$$

  where

  $$sig_{ERS} \coloneqq sig(sk_{ERS}, hash(Pw)) \quad and \quad sig_{VS} \coloneqq (sk_{VS}, sig_{ERS}).$$

  The thus a signed electoral register shall be installed on the register system. The whole electoral register is further signed with sk_{ERS}. This signed register should then be stored in case the need for validation arises.
- Once all components are online, the election is waiting to start. A configurable number of committee members must approve the start of the election in the committee-tool under their respective logins. Once this has happened, the system is awaiting passphrase authorization.
- For each of Polyas' components there will now be two remote access tokens (passphrases) in existence, which will have to be entered before the respective system will be operational. For the committee-tool, these shall be entered separately. When the committee tool is online and the start has been authorized, the tool will provide an interface for the committee to enter the respective passphrases of each other component.
- Once the last passphrase has been entered, the election enters the voting phase.

Voting The high level protocol of a voter casting a vote is described in figure 2. It is distinctive in several ways: For one, the vote is already sent to the ballot box server after the first acknowledgment. Then, the exact sent vote is sent back to the voter for verification. Thus the voter can be sure the ballot box server has interpreted his vote correctly. Votes are generally stored in an encrypted and signed manner.
Moreover, the tokens are also stored, encrypted using the public key of the involved database. Note that, according to the requirements of the protection profile, the token is explicitly not stored in the database when it is first sent to the ballot box server. It is only after the voter has confirmed his vote to be cast that the vote is finally written to the database.

Aside from the requirements of the protection profile and the signing and encryption of each individual vote, each block of thirty votes (whilst thirty is a variable) will be stored alongside with a signature of this block, factoring in the signature of the previous block, in the case that more than thirty votes have already been stored, providing a further layer of protection against any possible manipulation.
The voting token represents the authentication of the voter to the ballot box, so the ballot box cannot link the incoming or already cast vote to the credentials of the voter who issued the vote. An attacker attempting to break Polyas' anonymity would have to have unencrypted access to both of the fully separated systems (electoral register and ballot box) to establish such a link. Additionally, the vote token is encrypted via RSA, so the attacker would have to know the private key of the ballot box and/or electoral registry server in order to intercept it. Note that at no time will the token be written to the database. After the voting token is marked as invalid, its acquired memory is overwritten with pseudorandom values to ensure secure deletion.

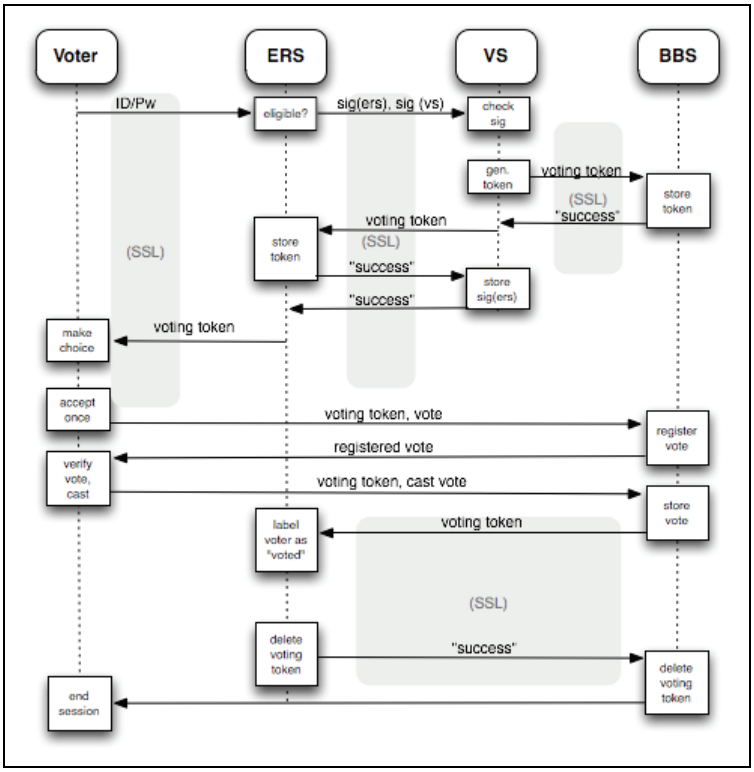


Figure 2: Polyas Protocol

To provide a means of defense against so-called phishing attacks, Polyas uses a module based on Image-Maps, presenting the user with a virtual, clickable keyboard on screen. There, the user can enter his credentials and the browser will only submit X/Y-coordinates. Because these are randomized with every different login-attempt, the risk of password phishing is drastically reduced.

The protection profile requires a voter be able to cancel his voting process as well as be able to intentionally cast an invalid vote. Both requirements are fulfilled. If the voting process is intentionally cancelled or technically interrupted before the vote is committed, no vote will be stored in the database, and the voter will be able to vote again. If the process is interrupted once the vote has been finally cast, the voter will be notified of his cast on his next login-attempt.
We consider the protocol to be safe against the voter trying to sell his vote. The possibility of selling would imply there being proof of his vote (and its content). Aside from the so far not solvable dilemma of remote voting, namely, that the voter can be observed throughout the entire voting process (see [KV05]), it is not possible for the voter to review his vote once cast. Therefore, it is also not possible to prove the contents of his vote to a third party after having submitted the vote and/or before submitting, since the voter might always change his choice shortly before finally casting his vote. Once the vote is cast, the voter will only be presented with the message that he has indeed voted, but for said reason no further details on his vote will be given.

Post-Voting To close the election, the committee has to issue the command to stop in the committee-tool. Once a sufficient number of "stop election" commands to satisfy the separation of duty has been cast, the committee-tool automatically walks through the process of stopping the election (see also [Me08]). For this purpose the validator server is first taken offline; thus disabling the possibility of further logons but not disturbing any possibly still ongoing vote processes.
After a certain amount of time to allow any remaining logged on voters to cast their votes, e.g., ten minutes, has expired, the electoral registry server is also taken offline, thus cancelling any eventually ongoing vote processes.
The ballot box server is then issued a command to count the votes and store the result along with a signature as a certificate of authenticity. The signed result can be retrieved by the committee from the ballot box server and is also displayed in the committee-tool. The committee-tool further generates a post-voting documentation including the results of the count, the log files of all involved systems, an image of each respective database, and the electoral register. All of this data will be stored in a signed archive.
As the software has been signed in the pre-voting process, it should be verified in the post-voting process that the software is still carrying the same signature to exclude the possibility of unauthorized modifications.

3 Achieving and maintaining compliance

3.1 Assessing the challenges

The Polyas architecture and process as described in 2.2 and 2.3 already fulfilled many of the objectives presented by the common criteria protection profile [PP08], as was already suggested in [RJ07]. The practicality of the implemented solutions for non-political remote electronic voting had been proven as mentioned in the introduction and in [VK06].

For one example, the protocol used by Polyas offers a natural way of achieving secrecy and anonymity when voting by fully separating the systems responsible for authenticating the voter and receiving/tallying his vote and only maintaining linkage in the form of a secure token that will be deleted at the very moment the voter has cast his vote. Simultaneously, the objective to only allow legit voters, who are unmistakably identified, had already been achieved, as was the secrecy and integrity of messaging, and the so-called overhaste protection that ensures that a voter will not cast an irreversible vote in error.
There were however, unfulfilled requirements given by [PP08] concerning the handling of the committee's tasks and its separation of duty, as well as preventing the tallying of intermediate results by members of the committee.

3.2 Assumptions and strict conformance

The common criteria protection profile for remote electronic voting does make certain conditions about the operation of the voting system that may not be circumvented for the certificate to remain valid. These conditions include, among others (for a complete list, please see [PP08]):

- The initial data in the electoral registry is that which the committee has approved. No additional data is entered by any means.
- Every registered voter has successfully received his credentials.
- The surrounding technical environment and network will function correctly for the time of the election.
- The voter will not be observed while voting (see 2.3 on vote buying).
- The committee can be trusted and will only use the functionality provided by the target of evaluation.
- The voter will verify he is connected to the correct voting system before voting.
- Data that is not under the control of the target of evaluation will be deleted once the vote has been successfully cast.

These assumptions reduce the functionality to be implemented to achieve compliance to a subset that is provided exclusively by the Polyas system as the target of evaluation.
Additionally, the protection profile demands strict conformance, which essentially means that all of the requirements have to be fulfilled by the target of evaluation itself (here: Polyas) and not by any organizational means 'on top' of the actual software.

3.3 Achieving separation of duty for the committee

One of the main challenges presented by the protection profile was the implementation of strict separation of duty for the election committee. This has been achieved in Polyas by introducing a fourth system to the original three systems in [RJ07], encapsulating the full functionality that the election committee can and may use to administer and oversee the election. This is supported by the assumption that the committee is to be trusted to not use any other knowledge or method to manipulate the election (see 3.2).

The aforementioned system, the Polyas committee-tool, integrates smoothly into the Polyas election lifecycle. It allows for the committee to safely, easily, and traceably start and stop as well as count and archive the complete election. In addition, it allows the committee to oversee the election, monitor the state of every involved system, run self-tests, view the logging of all involved systems, and see how many votes have been cast up to the point of examination as well as how many voters have been marked as having voted. Anomalies in this case can thus easily be detected even while the election is still in an ongoing state, so the committee could decide upon measures to be undertaken in case of any discrepancies.
When the election is to be counted, the committee-tool provides the option of warning the committee if the number of cast votes falls below a configurable amount, thereby possibly endangering the anonymity of the cast votes.
The most prevalent feature of the committee-tool, though, is its rigorous enforcing of the separation of duty for the committee. For every election, the separation of duty count variable S with $S > 1$ may be configured to a size appropriate for the specific committee. The system will then only execute the functions of starting, stopping and/or counting the vote once S different committee members have authorized this particular function with their respective credentials.
Once a committee member has given his or her authorization for a task (i.e. starting the voting phase), the committee-tool will inform him on the number of additional authorizations needed until the requested action will be carried out by the committee-tool. Every committee member may, of course, authorize each action once and only once.

3.4 System Safety and Self-Testing

The protection profile states that the election officers must be notified of malfunctions of the network connection or of storage of data. In such cases, the election officers should carry out a test sequence provided by the target of evaluation as demonstration of the correct operation (self-test) [PP08].
This requirement was achieved by including an already mentioned self-test routine in the committee-tool. This routine can either be carried out manually on request of an election officer, whereby it is ensured that only one self-test routine can be issued at once in case of multiple logged in election officers at the same time, or can be configured to run on a time-based schedule. In case of any detected faults at the levels of each system's hardware, storage integrity, system-time, anomalies in number of cast votes or network connection, the committee will immediately be notified of the fault and any possible consequences for the election and be asked to take appropriate counter-measures.
Any noticeable problems during the aforementioned self-test routine will be logged alongside with timestamps and therefore be included in the election archive documents.

3.5 Prevention of intermediate results

The protection profile requirement that no information flow between the committee and the ballot box server may result in intermediate results to be extrapolated in any way ([PP08]). Because the protection profile is formulated under the assumption that (see 3.1) the committee will only use the means provided by the target of evaluation itself, and because the committee usually will not have any direct access to the ballot box server, restricting the acting possibilities of the committee during the voting phase can solve this.
Once the vote has been started, there is no possibility offered in Polyas for the vote to be tallied unless the election is also stopped in the process. While the committee may oversee how many votes have been cast at every point in time during the voting phase, no disclosure on the content of these votes is ever given before the vote is finally stopped. Note that once stopped, in accordance to the protection profile, the election may not be resumed. Restarting a stopped election will unavoidably require the ballot box server to be cleared of any votes that had so far been cast.
Further, the stopping of the election as well as an assumed restart would have to be authorized by each of the S members of the committee, hence would not go unnoticed by at least S members of the committee as well as the voters who will be trying to vote during the—should such an attempt be made—inevitably resulting down-time of the voting system.

3.6 Audit records for the committee

The protection profile requires the committee to be able to read the audit information (successful identification and authentication of election officers, starting and stopping of the polling phase, starting of the tallying with determination of the election result, performance and results of every self-test and identified malfunctions) from the audit records of each involved system [PP08]. This information is made available in Polyas by means of the committee-tool, where each committee member can inspect the logs of each of the four Polyas component-systems in an easily readable and comprehensible format. Note that these audit files explicitly do not contain any information on the voters' logins, the identities of voters who have or have not cast their vote nor any vote content so no conflict arises with the given security objectives, particularly the secrecy of voting.

4 Conclusion

In this paper, we presented possible solutions to the challenges presented by the common criteria protection profile for remote electronic voting systems using the example of the Polyas system. The first look in respect to the then upcoming protection profile in 2007, [RJ07], still presented some challenges to overcome regarding the compliance of a state-of-the-art electronic voting system to the requirements of the common criteria protection profile. Additionally, there was no proof of the practicality of [PP08] so far.

The final version of the protection profile, by implying strict conformance, made organizational solutions a non-option. Instead, each requirement of the protection profile had to be directly implemented into the voting system. To achieve compliance for the Polyas system, certain minor adjustments to the protocol were necessary; as was a new tool for the committee to restrict its action options, its monitoring of the voting system's health, its view of the audit records, to enforce a separation of duty among committee members, and to prevent the tallying of intermediate results. As has been described, all of those objectives could be fulfilled while still maintaining strict conformance as well as preserving the advantages of the originally implemented protocol concerning secrecy of voting and the one-voter one-vote principle. An architectural balance between anonymity and security is still maintained in a sufficient manner for non-political remote electronic voting.

At present, we consider the described system to be compliant with the current protection profile and are looking toward qualified evaluation to achieve independently certified remote electronic voting. Therefore, we are confident that we have shown that it is possible to implement an electronic voting system for non-political voting systems that fulfill the criteria given by [PP08].

The [PP08] certification will be the first of its kind in the world of pc-based remote voting. The common criteria process will assure consistent and trusted evaluation, as well as opening up possibilities to further build upon attained knowledge and extend the acquired solutions. We look forward to additional challenges presented by the certification and publishing the first practical common criteria security target based on the protection profile.

Bibliography

[Gr06] Grimm, R., R. Krimmer, N. Meißner, K. Reinhard, M. Volkamer, and M. Weinand. 2006. Security requirements for non-political Internet voting. In *Electronic voting 2006. Proceedings of the 2nd international workshop on electronic voting,* ed. Robert Krimmer, 203–212. Bonn, Germany: Gesellschaft für Informatik.

[Me08] Menke, N. 2008. Sicherheit elektronischer Wahlsysteme am Beispiel des Online-Wahlsystems Polyas. Master's thesis, University of Kassel, Germany.

[PP08] Bundesamt für Sicherheit in der Informationstechnik. 2008. *Common Criteria Schutzprofil—Basisansatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, BSI-CC-PP-0037*

[RJ07] Reinhard, K., and W. Jung. 2007. Compliance of POLYAS with the BSI protection profile. Basic requirements for remote electronic voting systems. In *E-voting and identity. First international conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, revised selected papers, ed. Ammar Alkassar and Melanie Volkamer, 62-75*. Springer.

[KV05] Krimmer, R., and M. Volkamer. 2005. Bits or paper? Comparing remote electronic voting to postal voting. In: *EGOV (Workshops and Posters)*, 225–232.

[VA07] Volkamer, M., and A. Alkassar (eds.). 2007. *E-voting and identity. First international conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, revised selected papers.* Springer

[VK06] Volkamer, M., and R. Krimmer. 2006. Die Online-Wahl auf dem Weg zum Durchbruch. *Informatik Spektrum* 29 (2): 98–113.

A Survey: Electronic Voting Development and Trends

Komminist Weldemariam and Adolfo Villafiorita

Fondazione Bruno Kessler,
Center for Scientific and Technological Research (FBK-IRST)
via Sommarive 18
I-38050 Trento, Italy
(sisai, adolfo.villafiorita)@fbk.eu

Abstract: Any practitioner working on electronic voting (e-voting) seems to have different opinions on the main issues that seem to affect the area. On the one hand– given the criticality and the risk e-voting systems potentially pose to the democratic process–e-voting systems are permanently under a magnifying glass that amplifies any glitch, be it significant or not. On the other hand, given the interest e-voting raises within the general public, there seems to be a tendency to generalize and oversimplify. This tendency leads to attributing specific problems to all systems, regardless of context, situation, and actual systems used. Additionally, scarce know-how about the electoral context often contributes to make matters even more confused. This is not to say all e-voting systems show the security and reliability characteristics that are necessary for a system of such a criticality. On the contrary, a lot of work still has to be done. Starting from previous experiences and from a large-scale experiment we conducted in Italy, this paper provides some direction, issues, and trends in e-voting. Getting a clearer view of the research activities in the area, highlighting both positive and negative results, and emphasizing some trends could help, in our opinion, to draw a neater line between opinion and facts, and contribute to the construction of a next generation of e-voting machines to be safely and more confidently employed for elections.

1 Introduction

The advantages that e-voting systems can bring cannot be achieved without an observable cost (e.g., risks). One of which is opening up security vulnerabilities to attackers [Mer01, GGR07, BBC+08, BBC+10]. In that respect, recently we have seen that most currently deployed e-voting systems share critical failures in their design and implementation, which render their technical and procedural controls insufficient to guarantee trustworthy voting [LKK+03, KSRW04]. The lack of trust can also render even more secure and more reliable e-voting systems completely useless.

Clearly, the abundance of security threats in e-voting systems and their increasing popularity make a strong case for the need to propose new designs, protocols/schemes, techniques and tools for their design, development as well as their security assessment. The application and use of known techniques such as business process modeling and formal techniques and tools in voting, in general and in the development of an e-voting solution in particular, however are very limited and unsatisfactory. Additionally, work to

rigorously define e-voting properties and attack models and languages to describe the counter-measurements is still more preliminary.

Although some progress has been made in understanding and supporting the better development of e-voting systems, e.g., [MN03, XM05b, XM07, WVM07, VWT09, DKR09], there is no classification to understand the common characteristics, objectives, and limitations of these approaches. Thus the lack of a comprehensive comparative study provides little or no direction on choosing the appropriate development techniques for particular needs.

In this paper, we classify the most important development approaches for e-voting systems and compare them with respect to motivations, methods, and logic. More specifically, we have classified them in four major categories, according to what we believe to be their major contributions to the development of e-voting systems: UNDERSTANDING (the risks posed by the introduction of e-voting systems in the polling stations), REQUIREMENTS (developing requirements for e-voting), IMPLEMENTATION (designing voting schemes, protocols, and/or techniques), and ASSURANCE (using techniques and tools to analyze the security of existing systems, by giving lower-level and higher-level assurances). We hope the work contributes to the work done by designers, developers, certification authorities, as well as technical election officials.

The paper is organized as follows. In Section 2 we review the use of (business) process modeling and redesigning to understand the context and risks caused by the introduction of electronic solutions in the polling stations. In Section 3, we briefly survey the progress made in developing requirements for e-voting systems. We continue, in Section 4, by briefly surveying progress made in designing and implementing voting schemes. In Section 5, we focus on the application of formal methods and techniques and tools to assess the security of e-voting systems. We conclude, in Section 6, by presenting some conclusive considerations and viewpoints.

2 Understanding Risks

Understanding the "context" of elections is very important prior to introducing e-voting solutions. The obvious reason is that this helps to understand and discuss the possible risks that can result through the introduction of a new system. Previous work in this area focused on the understanding, representation, and effective implementation of e-voting procedures. That is, using business process reengineering (BPR) to understand what changes could be introduced to the conventional voting procedures to allow a safe and secure transition to electronic elections.

The BPR concept pertains to the redesign in the context of existing business rules, such that the introduction of e-voting solution can be evaluated. As it is critical to define roles and responsibilities within the e-voting process which could furnish a better understanding of who is responsible for doing what during the different process stages to

produce election results, it is also equally important to provide systematic methodology to deduce what could go wrong during this procedural rich workflow, instead of detecting the weaknesses well after attacks have already been taken.

As far as we are aware, the first use of BPR to evaluate the transition to e-voting is that proposed by Xenakis and Macintosh in [XM05b, XM07]. The authors investigated the need for business process reengineering to be applied to electoral process in order to propose a possible transition to an e-voting system. Risks and difficulties while introducing e-voting solutions are discussed, in more detail, in [XM04a, XM04b]. Furthermore, the same authors in [XM04c, XM05a] discussed the need for procedural security in electronic elections and provided various examples of procedural risks which occurred during trials in the UK. The approach can obviously highlight some of the security implications of the administrative workflow in e-voting, such as those discussed in [LKK+03]. However, these approaches do not provide techniques to systematically model and analyze procedural alternatives for better electronic solutions. Additionally, they do not provide ways to analyze the security aspect of these procedures. In other words, a systematic analysis of procedures is absent.

In references [Mat06, WVM07], the authors developed a UML-based methodology for modeling and analyzing electoral processes. The methodology is supported by a tool named VLPM [CMV09] that helps in the modeling, analysis and structuring of electoral procedures as business process models. Beyond that, the VLPM tool helps to assist a lawmaker to link laws with the process models, and a process engineer to analyze the effects of the changes due to the introduction of a new law (or law modification) on the models to maintain the "*synchronization*" of laws with models, as the same time by fostering collaboration between them, i.e. lawmaker and the process analyst. The methodology and the tool have been demonstrated for the development of an e-voting system named ProVotE [VWT09]. An approach to reason on security properties of the "*to-be"* models (which are derived from "*as-is*" model) in order to evaluate procedural alternatives in e-voting systems is presented [BDF+09]. In particular, using Datalog and the underlying analysis tool the authors expressed and analyzed security concerns, such as delegation of responsibility among untrusted parties and trust conflict. The aim is that of understanding problematic trust/delegation relationships and eventually finding ways to adopt a solution to the detected security properties violations.

3 Developing Requirements for E-voting

There are various international documents such as the recommendations from the European Union (EU) Venice Commission [Cou04] and the U.S. Federal Election Commission (FEC) Voting Systems Standard (VSS) [Fed02, Fed05], which describe a set of principles for voting systems. These documents mainly specify principles about the behaviors of each component of a voting system that should be respected, as well as the related procedures. The FEC-VSS, for instance, provides details about the standards to be used for performance and tests of voting machines. It also describes non-functional requirements (e.g., audits log features) and specifications for various hardware components. However, these kinds of requirements often make the development and

implementation of the actual system difficult. Moreover, the way these documents describe (security) requirements is hard to understand, and sometimes they contain contradicting/conflicting requirements —specifically, the conflict between the requirements for secrecy and accuracy. If the e-voting system needs to be developed in a safe and secure way, there must be an appropriate requirements definition. We have surveyed dozen works in this area. Because of the limited space, however, we are able to present but a few of those that we think are the most important and complete.

Reference [Mer01] presents a thorough discussion on three gaps that must be comprehended prior to developing (security) requirements for e-voting systems. These gaps are the *technological gap* —that is, between hardware and software, the *socio-technical gap* —that is, between social and computer policies, and the *social gap* —that is, between social policies and human behavior. The same author also coined the term audit trails, which is often used in DRE machines. Namely, the type of DRE equipped with printed audit trails is often called DRE-VVPAT. That is, a touch-screen-based machine that produces a printout of each vote, verified directly by the voter, to maintain a physical and verifiable record of the votes cast. Thus an essential activity to ensure e-voting system behaves correctly is to lay down what behaving correctly means for that system. This cannot be achieved without a proper engineering approach, such as requirements engineering techniques.

The author in [McG08] presented an approach to address the mentioned problems by proposing a methodological approach for analyzing the root causes of the conflicts, organizational barriers (or procedural barriers), and requirements of a critical election. The approach comprises of two strategies for the development of requirements, namely, top-down and bottom-up. The first one is aimed at developing a set of requirements from an existing catalogue. The latter, instead is aimed at developing a new catalogue.

Subsequent to [McG08], Volkamer has provided, "*a standardized, consistent, and exhaustive list of requirements for e-voting systems*" [Vol09]. Specifically, these requirements are mostly for standalone DRE and remote e-voting systems. Such requirements not only describe requirements that the system should meet, but also specify the corresponding laws or regulations for the evaluation of the systems themselves. The author developed a methodology for the requirement development process. The results of the methodology include system requirements (divided into functional, security, and usability requirements), organizational requirements, and assurance requirements for both stand-alone DRE voting machines and remote e-voting systems. Furthermore, the methodology comprises of crosschecks, existing catalogues, election principles, and the possible threats. This could allow software engineers and developers to easily understand how their systems meet these requirements. Following that, the author proposed an evaluation and certification procedure mostly for remote voting systems by complementing the Common Criteria common evaluation methodology and also developing a protection profile for remote voting.

In reference [WMV09], the authors showed the management and structuring of requirements using finite state machines (FSMs). That is, by defining relationships between requirements and system architecture based on FSMs. More specifically, the

methodology they followed allowed them to understand the election processes, identify constraints, and distinguish both common and event specific requirements from various requirements sources, e.g. from those mentioned above. These are then refined into fine-grained requirements using FSMs. The decomposition from high-level to low-level requirements and the logical dependencies among them have been demonstrated. Additionally, the separation between generic and election or configuration specific requirements is concrete and detailed enough to function as a general reference schema that could be adopted by other solutions. In other words, this approach is fairly general to be used for other e-voting systems and, possibly, to provide a roadmap —rough and draft as it might be— for bridging the gap between higher-level principles and lower level system specifications.

4 Designing Voting Schemes and/or Protocols

Prior works with respect to this area focused on the design of cryptographic schemes, protocols, and/or techniques to improve the design of voting machines. The ultimate goals of these approaches include ensuring a voter can be certain that her/his vote has been recorded correctly and accurately (*voter verifiability*), no voter can prove to anyone else how s/he voted (*receipt freeness*), and an independent body can verify that the recorded votes match exactly with the published tally after the election [Ive91, CFSY95, Cha04]. What is most common to all these approaches is that they rely on the underlying crypto- graphic principles to various degrees of complexity.

PunchScan [CPS+07, ECCP07] is a cryptographic voting system that is easy to use by the voter as well as by election officials, while at the same time providing a transparent and reliable process. It also provides public verifiability, election integrity and enhanced voter privacy. Scantegrity [CEC+08, CCC+09] is a successor of PunchScan that meets industrial standard by providing end-to-end verifiability of the integrity of critical steps in the voting process and election results. Prêt á Voter (verifiable electronic elections) [RBH+09] is a type of electronic voting system that uses paper based ballot forms that are converted to encrypted receipts to provide security and "auditability", at the same time remaining coercion resistant and easy to use. The Scratch & Vote is another cryptographic voting method proposed in [Adi06]. It provides public election "auditability" using simple, immediately deployable technology. The method combines a variety of existing cryptographic voting ideas such as homomorphic encryption —e.g., which allows votes to be tallied without decrypting individual votes, the cut-and-choose at the precinct approach, and so on. Additionally, works like [FOO93, BT94, RRN01, SCM08] attempt to provide (maximum) secrecy and/or anonymity for the vote and voter.

We cannot, however, say that cryptographic schemes and/or protocols address the current situation in the democratic process for several reasons. For example, the protocols that have been proposed so far do not yet overcome all of the barriers to their use in critical elections [McG08]; although DRE machines are very popular in public elections in some U.S. states, the applicability and scope of the proposed schemes are very limited in these machines. Moreover, as noted in [KSW05], some cryptographic

protocols have some security holes, such that sensitive information about the election can be leaked in one way or another. Therefore, we must analyze their security by considering the system in its entirety since these protocols are only one part of a larger system composed of voting machines, software design and implementations, and complex election procedures [KSW05].

In reference [Sas07], the author presents the concept of "*designing voting machines for verification,*" aimed at providing techniques to help vendors, independent testing agencies, and others verify the critical security properties of DRE voting machines. The basis idea of the approach consists of two interesting techniques. The first focuses on creating a trustworthy vote confirmation process, where the author proposed an architecture that splits the vote confirmation code into separate modules whose integrity are protected using hardware isolation techniques. The second focuses on helping to ensure a very important property in voting, that is, "*None of a voter's interactions with the voting machine, including the final ballot, can affect any subsequent voter's sessions.*" In order to do that, the author used a hardware resets technique that restores the state of modules components to a consistent initial value between consecutive voters. With this, it could be possible to eliminate the risk of privacy breaches and ensure that all voters are treated equally by the systems.

Other works, such as [SKW06, Yee07] apply techniques used in other domains —like pre-rendering user interface and hardware separation— to build higher assurance with accessible, verifiable and secure e-voting systems. The design of a trustworthy DRE-based voting system by exploring the TPM (Trusted Platform Module) infrastructures (e.g., PKI, hardware protection of cryptographic keys) is presented in [PT09]. Additionally, the authors present a scheme that improves registration integrity, and introduces a design that prioritizes election integrity. Their voting system has nine steps as a whole, from an election's inception to its final conclusion.

5 Providing Assurances

With respect to the assurance of e-voting systems, existing works focus on two main areas to assess the security of e-voting systems. While the first one focuses on providing lower-level assurances, the other focuses on providing higher-level assurances; both use powerful techniques and tools.

5.1 Applying formal methods to e-voting

The use of formal methods in the specification and verification of e-voting systems is relatively new. Existing works in this area present formal specification and verification of an e-voting system at different levels of abstraction. These works aim to demonstrate how feasible the formal verification of voting machine logic, thereby providing a higher level of assurance about the security of the system. In this area the trends focus on three

closely related aspects, mainly according to the aim of the verification. These are verifying cryptographic protocols, system behavior, and procedures.

The references [DKR09, KR05] present a framework for formal specification and verification of three privacy-type e-voting protocol properties. These properties are vote-privacy, receipt-freeness, and coercion-resistance. The authors used applied π-calculus [AF01] to formalize these properties as observational equivalence, after formalizing the voting protocol as a set of processes using the same machinery. In [CFM+08], the authors used a CCS (Calculus of Communicating Systems)-like process algebra with cryptographic primitives to specify and analyze some properties of the e-voting system they built. More specifically, they presented a small mobile implementation of an e-voting system named M-SEAS (Mobile Secure E-voting Applet System) and used formal verification technique to validate the security properties of the system.

The authors in [VWT09] demonstrate the integration of formal methods in the development process of a voting system. In particular, the authors specified the behaviors of voting control logic using a UML finite state machine and developed a tool named FSMC+[1] that automatically generates NuSMV [CCG+02] code corresponding to the specified FSM (this helped the requirements discussed in [VWT09]). Then they performed the verification using the NuSMV model checker. The results of the model checker, presented in the form of counter-measurement, are then analyzed. This enabled the authors to incorporate the analysis results of the verification into the actual development process of the core application.

In references [WKV09, WKV10], the authors show how formal methods can be used to reverse synthesize existing e-voting systems (named ES&S voting systems). They used the ASTRAL language to specify the ES&S voting process and used the PVS analysis tool. A number of critical security requirements that the machines should respect have been specified and analyzed against the specification. Subsequently, the authors specified known attacks against the system (as demonstrated in [MBV07]) using the same machinery and extended the original specifications, and then preformed the analysis on the extended model with the same set of critical security requirements that the original specifications should respect. The two main lessons drawn from their work are: formal methods help gain a better understanding of the security "boundaries" of e-voting systems, and the role that open specifications play in the development of more secure e-voting systems.

The reference [SJSW09] presents an approach for designing and analyzing of an e-voting machine based on a combination of formal verification and systematic testing. They formally verify the correctness of each of the individual components of the voting machine, as well as verify some of the crucial correctness properties of their composition. Their work is targeted to the following verification goals: ensuring that each individual component of the voting machine and their composition should meet the specification of the individual components and their composition respectively; voting machine should be structured to enable sound systematic system testing; ensuring that

[1] http://ict4g.fbk.eu/fsmcp/last/

the voting machine must behave and store votes according to the voters selection when configured with a particular election definition file. For each module, they construct a formal specification that fully characterizes the intended behavior of that component. A number of properties related to the structural and functional aspects that the machine should satisfy are identified and specified. They used Verilog [TM91] for the implementation of their specification and SMV[2] analysis tool and "satisfiability" solving (especially, the SMT solver) to verify that their Verilog implementation meets the specifications.

Finally, in reference [WV08], the authors proposed an approach to formally analyze procedures. Namely, they proposed a methodology based on the NuSMV [CCG+02] machine to analyze procedures systematically.

5.2 Assessing exiting e-voting systems

Some e-voting systems currently deployed in elections have recently undergone a thorough and independent scrutiny to evaluate their security and quality. This is because, in recent years, the DRE machines raised serious security concerns. These machines make the election process less verifiable and greatly expand the aspects of an election for which voters must rely solely on trust. Security vulnerabilities have been reported in each aspect of security—that is, technological, socio-technical, and social aspects, as noted prior in [Mer01]. These vulnerabilities have been systematically investigated and proved by various academic studies. This creates an enigma in the trustworthiness of the machine and the voting process as well.

In line with this, we mention the following academic researches [Jon03, KSRW04, GGR07, BBC+08, ASH+08]. These works assess both hardware and software of different forms of e-voting machines (e.g., Diebold/Premier, ES&S, InterCivic), mostly used in some U.S. states. The studies identified serious design and implementation flaws, which are notable for their level of egregiousness. More specifically, these analyses have showed that the current e-voting systems are vulnerable to very serious attacks. In addition, they have produced a catalogue of vulnerabilities and possible attacks. Some analyses also suggested a drastic change in the way in which e-voting systems are designed, developed, and tested (e.g., by identifying procedures to eliminate or mitigate the discovered issues, by developing a precise methodology and toolsets for the assessment). The assessment methodology presented in [BBC+08, MBV07] is particularly astonishing as it provides various insights on each individual and in-depth step of the analysis. The software testing community can use it for the evaluation of other complex-security critical systems and evaluation.

[2] http://www.kenmcmil.com/

6 Discussions and Conclusion

There are a number of established approaches for modeling, specifying, and verifying a system satisfies a set of properties. One important contributor to the security of any system is the way in which the software is designed and developed. Standards for software engineering developed over the last forty plus years require that a system undergo a rigorous process of requirements definition, structured design and review, and careful programming and testing [Som95]. Like proper engineering leads to cars of higher quality, so too does better software engineering lead to more secure, robust software computer systems. Systems that are designed without this kind of careful design and implementation are almost certain to have flaws and security issues.

BPR techniques help to understand, model, and analyze the high-level context of the electoral processes. This provides information about the context of the business architecture (*as-is*) and software delivery (*to-be*) prior to the subsequent development activities for the introduction of an e-voting solution. It also helps in assessing the effectiveness of the processes as experienced and evaluated by the citizens outside the development and support organizations. However, it is not always possible to transform a business solution into an e-voting solution [AO05]. This is because, unlike business processes, the electoral processes are tightly bounded by legal frameworks and are usually more regulated than business processes. Thus, we need a proper methodology and tools that abet such reengineering activities. However, some approaches such as the one given in [CMV09] can be a starting point to extend and reuse in the reengineering process of e-voting projects.

The use of formal methods has been shown to improve the security and quality of complex systems. These approaches allow designers to prove, test, or otherwise examine interesting properties of a complex process whose behavior is specified abstractly, and then interactively refine the behavioral specification to be as close to an implementation as appropriate for a given assurance level. In practice, moreover, the technique has been recognized as a powerful and effective mechanism for improving the security and quality of complex systems (e.g., in avionics). Thus, drawing a direct connection to this can help to improve the current development trends of e-voting machines.

Moreover, the studies of experimental data about the e-voting machines' security, performance and their evolution with respect to the social and technical aspects are still unsatisfactory. This limits their use on a larger scale. For example, data sets based on observing security threats to voters' anonymity by following standard procedures that illustrate each machine's behavior during elections can help raise the transparency in elections using electronic devices and increase the confidence of voters in the democratic system. Data sets related to the process of setting up experiments, running an election, and performing security evaluations across various voting machines (e.g., as in Diebold and ES&S) provide information about the behavior of machines under malicious circumstances, whether they are designed carefully or not, and provide recommendations that need to be considered for design alternatives.

Developing and deploying e-voting systems in a safe and secure manner requires ensuring the technical and procedural levels of assurance with respect to social and regulatory frameworks. In this paper, we have presented techniques mainly in three areas (namely, BPR, formal methods, and security) and showed how these techniques are effectively exercised for correct design and implementation of e-voting systems. Therefore, the success of the next generation of e-voting machines depends upon being able to capitalize one the lessons learned from different disciplines. The work we have presented in this paper is one way in which we can get a better understanding of the strengths and the weaknesses of existing techniques and thus lay the foundations for engineering, designing, implementing, as well as deploying a new generation of more secure and robust technologies for polling stations.

Bibliography

[Adi06] Adida, Ben 2006. Advances in cryptographic voting systems. PhD diss., Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology..

[AF01] Abadi, Martín, and Cédric Fournet. 2001. Mobile values, new names, and secure communication. *SIGPLAN Not* 36(3):104–115. New York, NY, USA: ACM.

[AO05] Alpar, Paul, and Sebastian Olbrich. 2005. Legal requirements and modelling of processes in e-government. *Electronic journal of e-government*, 3.

[ASH+ 08] Ansari, Nirwan, Pitipatana Sakarindr, Ehsan Haghani, Chao Zhang, Aridaman K. Jain, and Yun Q. Shi. 2008. Evaluating electronic voting systems equipped with voter-verified paper records. *IEEE Security and Privacy* 6(3):30–39: IEEE Computer Society.

[BBC+ 08] Balzarotti, Davide, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard Kemmerer, William Robertson, Fredrik Valeur, and Giovanni Vigna. 2008. Are your votes really counted?: Testing the security of real-world electronic voting systems. In *ISSTA '08: Proceedings of the 2008 international symposium on software testing and analysis*, 237–248. New York, NY, USA: ACM.

[BBC+10] Balzarotti, D., G. Banks, M. Cova, V. Felmetsger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna. 2010. An experience in testing the security of real-world electronic voting systems. *IEEE transactions on software engineering*.

[BDF+09] Bryl, Volha, Fabiano Dalpiaz, Roberta Ferrario, Andrea Mattioli, and Adolfo Villafiorita. 2009. Evaluating procedural alternatives: A case study in e-voting. *EG* 6(2):213– 231.

[BT94] Benaloh, Josh, and Dwight Tuinstra. 1994. Receipt-free secret-ballot elections (extended abstract). In *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on theory of computing*, 544–553. New York, NY, USA: ACM.

[CCC+ 09] Chaum, D., R.T. Carback, J. Clark, A. Essex, S. Popoveniuc, R.L. Rivest, P. Ryan, E. Shen, A.T. Sherman, and P.L Vora. 2009. Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes. *IEEE transactions on information forensics and security* 4(4):611–627.

[CCG+02] Cimatti, Alessandro, Edmund Clarke, Enrico Giunchiglia, Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani, and Armando Tacchella. 2002. NuSMV 2: An open source tool for symbolic model checking. In *Computer aided verification, lecture notes in computer science*, 241–268. Berlin / Heidelberg: Springer.

[CEC+ 08] Chaum, David, Aleksander Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, and Poorvi L. Vora. 2008. Scantegrity: end-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46: IEEE Computer Society.

[CFM+08] Campanelli, Stefano, Alessandro Falleni, Fabio Martinelli, Marinella Petrocchi, and Anna Vaccarelli. 2008. Mobile implementation and formal verification of an e-voting system. In *Proceedings of the 2008 Third International Conference on Internet and Web Applications and Services,* Washington, DC, USA: IEEE Computer Society.

[CFSY95] Cramer, Ronald J.F., Matthew Franklin, L. A.M. Schoenmakers, and Moti Yung. 1995. Multi-authority secret-ballot elections with linear work. Technical report, CWI (Centre for Mathematics and Computer Science).

[Cha04] Chaum, David. 2004. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy* 2:38–47: IEEE Computer Society

[CMV09] Ciaghi, Aaron, Andrea Mattioli, and Adolfo Villafiorita. 2009. VLPM: a tool to support BPR in public administration. In *Proceedings of the Third International Conference on Digital Society (ICDS2009)*, 289–293: IEEE Computer Society.

[Cou04] Council of Europe. 2004. Recommendation on legal, operational and technical standards for e-voting. Council of Europe, September. [Available online at https://wcd.coe.int/ViewDoc.jsp?id=778189]

[CPS+ 07] Carback, Richard T., Stefan Popoveniuc, Alan T. Sherman, and David Chaum. 2007. Punchscan with independent ballot sheets: Simplifying ballot printing and distribution with independently selected ballot halves. In *Proceedings of the 2007 IAVoSS workshop on trustworthy elections (WOTE 2007)*. [Available online at http://punchscan.org/papers/ibs_carback.pdf]

[DKR09] Delaune, Stéphanie, Steve Kremer, and Mark Ryan. 2009. Verifying privacy-type properties of electronic voting protocols. *J. Computer Security* 17(4):435–487.

[ECCP07] Essex, Aleks, Jeremy Clark, Richard Carback, and Stefan Popoveniuc. 2007 Punchscan in practice: An E2E election case study. In *Proceedings of the 2007 IAVoSS Workshop on trustworthy elections (WOTE 2007)*, held in conjunction with 7th workshop on Privacy Enhancing Technologies, Ottawa, Canada.

[Fed02] Federal Election Commission. 2002. Voting system standards. USA: United States Election Assistance Commission, http://www.eac.gov/.

[Fed05] Federal Election Commission. 2005 Voluntary voting system guidelines (VVSG). USA: United States Election Assistance Commission, http://www.eac.gov/.

[FOO93] Fujioka, Atsushi, Tatsuaki Okamoto, and Kazuo Ohta. 1993.A practical secret voting scheme for large scale elections. In *ASIACRYPT '92: Proceedings of the workshop on the fheory and application of cryptographic techniques*, 244-251. London, UK, 1993: Springer-Verlag.

[GGR07] Gardner, Ryan, Sujata Garera, and Aviel Rubin. 2007. On the difficulty of validating voting machine software with software. In *EVT'07: Proceedings of the USENIX/accurate electronic voting technology on USENIX/accurate electronic voting technology workshop B*erkeley, CA, USA: USENIX Association.

[Ive91] Iversen, Kenneth R. 1991. A cryptographic scheme for computerized elections. In *CRYPTO '91: Proceedings of the 11th annual international cryptology conference on advances in cryptology,* 405–419. London, UK: Springer-Verlag.

[Jon03] Jones, Douglas W. 2003. The evaluation of voting technology, chapter 1. In Advances in Information Security, 3–16. Ed. Dimitrius Gritzalis: Kluwer Academic Publisher

[KR05] Kremer, Steve, and Mark D Ryan. 2005. Analysis of an electronic voting protocol in the applied pi-calculus. In *Proceedings of the 14th European symposium on programming (ESOP'05), lecture notes in computer science*, 186–200. Edinburgh, U.K.: Springer.

[KSRW04] Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. 2004. Analysis of an electronic voting system. IEEE Symposium on security and privacy, 0:27: IEEE Computer Society

[KSW05] Karlof, Chris, Naveen Sastry, and David Wagner. 2005. Cryptographic voting protocols: a systems perspective. In *Proceedings of the 14th conference on USENIX security symposium* Berkeley, CA, USA: USENIX Association.

[LKK+ 03] Lambrinoudakis, Costas, Spyros Kokolakis, Maria Karyda, Vasilis Tsoumas, Dimitris Gritzalis, and Sokratis Katsikas. 2003. Electronic voting systems: Security implications of the administrative workflow. In *Proceedings of the 14th international workshop on database and expert systems applications*, 467, Washington, DC, USA: IEEE Computer Society.

[Mat06] Mattioli, Andrea 2005-2006. Analisi dei processi in ambito di voto elettronico per le elezioni in Provincia di Trento. Master's thesis, University of Trento.

[MBV07] McDaniel, P., M. Blaze, and G. Vigna. 2007. EVEREST: Evaluation and validation of election-related equipment, standards and testing. Ohio Secretary of State's EVEREST project report. [available online at www.cs.ucsb.edu/~vigna/publications/2007_mcdaniel_blaze_vigna_voting.pdf]

[McG08] McGaley, Margaret. 2008. E-voting: An immature technology in a critical context. PhD diss., Department of Computer Science, National University of Ireland, Maynooth.

[Mer01] Mercuri, Rebecca T. 2001. Electronic vote tabulation checks and balances. PhD diss., University of Pennsylvania.

[MN03] Mercuri, Rebecca T., and Peter G. Neimann. 2003. Verification for electronic balloting systems, chapter 3. In *Advances in information security,* 31-42: Kluwer Academic Publishers.

[PT09] Paul, Nathanael, and Andrew S. Tanenbaum. 2009. The design of a trustworthy voting system. *Annual computer security applications conference (ACSAC)*, 507-517: IEEE Computer Society.

[RBH+ 09] Ryan, P.Y.A., D. Bismark, J. Heather, S. Schneider, and Zhe Xia. 2009. Prêt á Voter: A voter-verifiable voting system. *IEEE transactions on information forensics and security* 4(4).

[RRN01] Ray, Indrajit, Indrakshi Ray, and Natarajan Narasimhamurthi. 2001. An anonymous electronic voting protocol for voting over the internet. In *WECWIS '01: Proceedings of the third international workshop on advanced issues of e-commerce and web-based information systems*, 188. Washington, DC, USA: IEEE Computer Society.

[Sas07] Sastry, Naveen K. 2007. Verifying security properties in electronic voting machines. PhD diss., EECS Department, University of California, Berkeley.

[SCM08] Santin, Altair O., Regivaldo G. Costa, and Carlos A. Maziero. 2008. A three-ballot-based secure electronic voting system. *IEEE Security and Privacy* 6(3):14–21: IEEE Computer Society

[SJSW09] Sturton, Cynthia, Susmit Jha, Sanjit A. Seshia, and David Wagner. 2009. On voting machine design for verification and testability. ACM conference on computer and communications security (CCS'09), Chicago, Illinois, USA, November 9-13 , 463-476: ACM

[SKW06] Sastry, Naveen, Tadayoshi Kohno, and David Wagner. 2006. Designing voting machines for verification. In *Proceedings of the 15th conference on USENIX security symposium,* volume 15. Berkeley, CA, USA: USENIX Association.

[Som95] Sommerville, Lan. 1995. Software engineering (5th ed.). Addison Wesley Lonman Publishing Co., Inc. Redwood City, CA, USA.

[TM91] Thomas, Donald E., and Philip R. Moorby. 1991. The VERILOG hardware description language. Norwell, MA, USA: Kluwer Academic Publishers.

[Vol09] Volkamer, Melanie. 2009. Evaluation of electronic voting: requirements and evaluation procedures to support responsible election authorities. Springer Publishing Company, Incorporated: Springer.

[VWT09] Villafiorita, Adolfo, Komminist Weldemariam, and Roberto Tiella. 2009. Development, formal verification, and evaluation of an e-voting system with VVPAT. *IEEE transaction on information forensics and security* 4(4) 651--661.

[WKV09] Weldemariam, Komminist, Richard A. Kemmerer, and Adolfo Villafiorita. 2009. Formal analysis of attacks for e-voting system. In *CRiSIS '09: Fourth international conference on risks and security of internet and systems*: IEEE.

[WKV10] Weldemariam, Komminist, Richard A. Kemmerer, and Adolfo Villafiorita. 2010. Formal specification and analysis of an e-voting system. In *The 5th international conference on availability, reliability and security (ARES 2010)*: IEEE Computer Society.

[WMV09] Weldemariam, Komminist, Andrea Mattioli, and Adolfo Villafiorita. 2009. Managing requirements for e-voting systems: Issues and approaches motivated by a case study. In *Proceedings of the first international workshop on requirements engineering for e-voting systems*: IEEE Computer Society.

[WV08] Weldemariam, Komminist, and Adolfo Villafiorita. 2008. Modeling and analysis of procedural security in (e)voting: The Trentino's approach and experiences. *In Proceedings of the conference on Electronic voting technology (EVT)*. Berkeley, CA, USA: USENIX Association.

[WVM07] Weldemariam, Komminist, Adolfo Villafiorita, and Andrea Mattioli. 2007. Assessing procedural risks and threats in e-voting: Challenges and an approach. In *VOTE-ID, lecture notes in computer science*, 38–49: Springer.

[XM04a] Xenakis, Alexandros, and Ann Macintosh. 2004. G2G collaboration to support the deployment of e-voting in the UK: A discussion paper. In *EGOV, lecture notes in computer science*, 240–245: Springer.

[XM04b] Xenakis, Alexandros, and Ann Macintosh. 2004. Levels of difficulty in introducing e-voting. In *EGOV*, 116–121: Springer.

[XM04c] Xenakis, Alexandros, and Ann Macintosh. 2004. Procedural security analysis of electronic voting. In *ICEC '04: Proceedings of the 6th international conference on electronic commerce*, 541–546. New York, NY, USA: ACM Press.

[XM05a] Xenakis, Alexandros, and Ann Macintosh. 2005. Procedural security and social acceptance in e-voting. In *HICSS '05: Proceedings of the 38th annual Hawaii international conference on system sciences (HICSS'05) - Track 5,* 118.1. Washington, DC, USA: IEEE Computer Society.

[XM05b] Xenakis, Alexandros, and Ann Macintosh. 2005. Using business process re-engineering (BPR) for the effective administration of electronic voting. *The electronic journal of e-government* 3(2) 91-98. [available online at www.ejeg.com]

[XM07] Xenakis, Alexandros, and Ann Macintosh. 2007. A methodology for the redesign of the electoral process to an e-electoral process. *International journal electronic governance* 1:4 –16.

[Yee07] Yee, Ka-Ping. 2007. Extending prerendered-interface voting software to support accessibility and other ballot features. In *EVT'07: Proceedings of the USENIX workshop on accurate electronic voting technology*, 5. Berkeley, CA, USA: USENIX Association.

Session 4: Operation and Evaluation of E-Voting Systems

An Evaluation and Certification Approach to Enable Voting Service Providers

Axel Schmidt[1], Melanie Volkamer[2], Johannes Buchmann[1]

[1]Cryptography and Computer Algebra
Technische Universität Darmstadt
Hochschulstr. 10
D-64289 Darmstadt
Germany
{axel, buchmann}@cdc.informatik.tu-darmstadt.de

[2]Center for Advanced Security Research Darmstadt (CASED)
Mornewegstr. 32
D-64293 Darmstadt
melanie.volkamer@cased.de

Abstract: In this paper we provide an evaluation and certification approach for Voting Service Providers (VSPs) which combines the evaluation of the electronic voting system and the operational environment for the first time. The VSP is a qualified institution which combines a secure voting system and a secure operational environment to provide secure remote electronic elections as a service [La08]. This centralized approach facilitates legal regulation and evaluation. So far, a legal regulation framework for VSPs has been developed which demands evaluation and certification of the VSP [Sc09a]. Therefore the VSP is required to provide a security concept in which it demonstrates satisfaction of the security requirements defined in the legal regulation. However neither the content of this security concept nor an adequate evaluation methodology has been specified so far. We therefore developed a security concept template and a comprehensive evaluation methodology for the VSP, which includes both the voting system and operational environment of VSPs. Our proposal incorporates existing evaluation methodologies to facilitate evaluation and certification. With this paper and the legal regulation a realistic approach to enable the VSP concept is accomplished.

1 Introduction

Security is one of the most important goals in the field of electronic voting. A lot of research has been done to develop sophisticated e-voting protocols with complex cryptographic mechanisms to improve security. An additional approach to strengthen security and trustworthiness is the evaluation and certification of e-voting systems.
Here the security functionality of a system is analyzed for compliance with a predefined and approved set of requirements. In 2008 the first evaluation standards for online voting systems were published–the "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products" [*sic*] [VV08].

However, in [Sc09b] the authors showed that the security of the operational environment, in which the voting system is implemented, has to be considered as well. One attempt to combine the security of a voting system with a secure operational environment is the Voting Service Provider (VSP) concept [La08]. The VSP is a qualified and professional institution which provides secure remote electronic elections as a service on behalf of the election host. Therefore the VSP provides the secure hardware and software, the voting system, the secure infrastructure as well as the specialist knowledge and the skilled personnel needed to operate electronic elections securely. The VSP is a centralized approach and thereby can be regulated and evaluated easily. Legal regulation is an important means to provide a basis for security, trustworthiness and correct behavior. A corresponding evaluation and certification procedure can verify the compliance with such legal regulation. In [Sc09a] the authors therefore introduced a legal framework for the regulation of VSPs. The framework defines requirements for VSPs and demands their evaluation and certification. The legal regulation stipulates that the evaluation and certification of VSPs is based on a 'security concept.' In this security concept, the VSP needs to demonstrate how the requirements of the legal framework are satisfied. The evaluation authority appointed in the statute uses the security concept as the basis for evaluation and certification of the VSP. The security concept comprises technical and organizational aspects, which have to be addressed by the voting system and/or the operational environment. Concluding, the centralized VSP concept and the legal framework provide an ideal basis for a combined evaluation of the voting system and operational environment.

However neither the content of the security concept for VSPs nor an adequate evaluation methodology has been specified so far. Therefore we developed a comprehensive template for such a security concept for VSPs. Further we propose a combined evaluation approach incorporating existing evaluation methodologies for both the voting system and operational environment. We expand the Common Criteria evaluation for online voting systems [VV08] by including an evaluation approach for the operational environment based on the approved *IT-Grundschutz/ISO27001*[1] methodology [G08d]. In this way we facilitate a fully comprehensive evaluation of VSPs and thereby enable the VSP to be put into practice. Our approach is practical since already existing certificates can be included in the evaluation thereby reducing costs and efforts of the VSP evaluation.

We consider related work in Section 2. In Section 3 we develop a security concept template as the basis for evaluation of VSPs. The template specifies which requirements need to be considered. In Section 4 we introduce the Common Criteria and *IT-Grundschutz/ISO27001* certification methodologies and show how they can be used in a security concept based VSP evaluation. In Section 5 we discuss the applicability of these certification methodologies to the VSP scenario and conclude the paper.

[1] eng.: IT Basic Protection/ISO27001

2 Related Work

In the area of e-voting, evaluation is mainly considered in the Common Criteria Protection Profile for online voting products [VV08], which we incorporated in our work. Its development has been discussed in [VKG07]. Several companies are striving to have their e-voting software certified accordingly, e.g. the Polyas voting software by Micromata [RJ07].
Regarding the operational environment, there exist several methodologies. For example, ITIL is a collection of best practices concentrating on IT service management and the optimization of service quality[2]. However, ITIL is less security-oriented. A Swiss project in Geneva is working on the implementation and evaluation of an e-voting system[3]. The coordinators specified security requirements for their voting system[4] and used the ISO27001 methodology for evaluation which is a standard for Information Security Management Systems (ISMS) [Re07, Tr09, Is08]. Our evaluation approach is more comprehensive since it builds on a specialized legal regulation and incorporates the Common Criteria Protection Profile [VV08], being the current evaluation standard for online voting systems, which we expand by using the *IT-Grundschutz*/ISO27001" methodology for evaluation of the operational environment. Thereby we extend the basic ideas of the Swiss approach. Weldemariam et al. provided a more theoretical approach to assess the operational environment of e-voting systems [WVM07]. In contrast, our work focuses on the practicability of the evaluation in real-world scenarios.
In Germany, the evaluation of Certification Authorities (CAs) is based on an approach similar to the VSP evaluation. The "German Signature Ordinance" legally regulates CAs and requires them to provide a security concept (see [G01] § 2). However profound information on the content of the security concept is missing thereby complicating the CA evaluation. To improve the situation for VSPs, we therefore developed a detailed security concept template facilitating VSP evaluation.

3 A Security Concept Template for Voting Service Providers

The legal framework introduced in [Sc09a] specifies only the basic structure of the security concept for VSPs. We therefore developed a detailed security concept template which contains all requirements a VSP must satisfy in order to comply with the legal regulation. We point out that the legal framework for VSPs was developed in Germany and therefore might need adjustment in order to be applied in other countries. This is considered future work.

[2] http://www.ogc.gov.uk/guidance_itil.asp
[3] http://www.ge.ch/evoting/english/welcome.asp
[4] http://unpan1.un.org/intradoc/groups/public/documents/Other/UNPAN022422.pdf

3.1 Methodology

To identify the requirements, which have to be considered by the VSP in the security concept to comply with the legal regulations [Sc09a], we deeply analyzed the legal framework including the act and ordinance. In order to facilitate the interpretation of the requirements by VSPs, we adapted these requirements to the technical field of application. To this end, we analyzed the corresponding preambles of the legal frameworks. They contain additional information which is relevant for implementation and thereby facilitate concretizing the legal requirements. Moreover we incorporated existing technical standards and requirements catalogs in order to further concretize and supplement the requirements from the legal framework. Therefore we utilized recent standards including the "Legal, Operational and Technical Standards for E-voting" from the Council of Europe [Co04], which define comprehensive requirements for electronic elections, as well as the catalog of requirements for the operational environment of electronic elections presented in [Sc09b], which is based on a multitude of existing literature on e-voting security. We used applicable requirements from these sources for adapting the legal requirements to the technical field and integrated them in our template. As a result many requirements from the catalog [Sc09b] and [Co04] have been included in the template. We structured the resulting requirements based on the provisions from the legal framework. Our approach and especially the incorporation of existing technical standards are inspired by the interdisciplinary KORA[5] methodology [Ha92]. KORA describes a procedure to derive technical requirements and implementation proposals from legal stipulations for the similar scenario of information and communication systems. It has been tried and tested many times (see for example [Ha94] and [Id00]).

3.2 Template Structure and Content

The legal framework provides a basic structure for the security concept. For our template we adjusted the structure slightly in order to merge related requirements. Due to space limitations, we cannot present the complete security concept template in this paper[6]. We present the structure and an overview of the included requirements. We provide detailed examples in Section 4.3.

Technical, structural and organizational safeguards: The VSP shall describe all technical, structural and organizational measures essential for the operation of a VSP according to the legal regulations. Here we incorporated the majority of requirements from the catalog [Sc09b]. The section includes requirements for secure communication channels that provide unaltered and confidential communication between the voter and election server. Secure storage media must provide integrity, availability, and sufficient capacity. Secure erasure of sensible data as well as archiving and system cleansing measures must be provided.

[5] *Konkretisierung Rechtlicher Anforderungen*, eng.: Implementation of legal requirements
[6] The complete template will be published as a technical report shortly.

The VSP must realize the management of cryptographic keys and certificates and correct time for all system components. The VSP shall prevent attacks and unauthorized access to the voting server. The VSP must ensure correct setup of the voting system, set and publish time tables and register the voters correctly.

Technical products for remote electronic elections: The VSP shall list the technical products used for its electronic voting services, e.g., electronic voting software or election server hardware. If a product is certified this should be indicated here.
Setup and operation of remote electronic elections: The VSP shall demonstrate how it achieves availability; confidentiality and integrity of the voting services and election data; and how it realizes the operation of the election, the briefing of voters, and election host. The VSP's voting services must fulfill the election principles of the particular type of election. It must achieve the secure identification and authentication of the voters. The VSP must demonstrate how the legal requirements for ballot casting are satisfied [Sc09a]. Integrity and verifiability of tallying must be accomplished. The VSP must show how the election and adherence to law are documented and how integrity protection and archiving of such data are achieved. The secure system state must be ensured. This includes correct initial state, secure system interruption, and closure of the voting phase. The VSP must ensure the secure delivery of authentication means to the voters and correct representation of the electronic ballot.

Warranty of data protection: The VSP is required to prove that the applicable legal data protection provisions, i.e., the German Federal Data Protection Act, the German State Data Protection Act, and the German Teleservices Act, were observed. This can be achieved by a data protection audit, e.g., by the German Independent Centre for Privacy Protection Schleswig-Holstein[7] or *IT-Grundschutz*, which provides a data protection module[8].

Guarantee and maintenance of operation: The VSP shall demonstrate the precautions taken to guarantee and maintain the operation of the electronic voting service, especially in case of emergencies.

Personnel: The VSP shall demonstrate that the employed personnel have the reliability (i.e., guarantee that the legal provisions regarding the VSP's operation are observed) and the specialist qualifications (i.e., the knowledge, experience and skills necessary for their work).

Residual security risks: The VSP must assess and value remaining security risks in order to evaluate its reliability. This relates to the residual risk of system failure or interruption in particular with regard to deployed technology. The VSP may refer to valuation from evaluation authorities or manufacturers of deployed products. We discuss this in Section 4.4.

[7] https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm
[8] https://www.bsi.bund.de/cae/servlet/contentblob/475580/publicationFile/31090/moduleb01005_pdf.pdf

4 Combined Evaluation Approach

The legal framework [Sc09a] for VSPs does not demand a specific methodology for evaluating the security concept. However the incorporation of existing evaluation certificates is explicitly allowed. The intention is to facilitate the evaluation process and avoid double checking. We show how this approach can be realized by applying two approved evaluation methodologies for both voting system and operational environment to the security concept evaluation. We analyzed the requirements contained in our security concept template and found that many requirements are satisfied by either a voting system certified according to the Common Criteria Protection Profile [VV08] or by safeguards for the operational environment from the *IT-Grundschutz/ISO27001* catalogs [G05]. To this end we compared both the 'objectives' of the Protection Profile and the 'modules' and safeguards from the *IT-Grundschutz/ISO27001* catalogs with the requirements from our template. We describe this in more detail in the following sections. By utilizing an accordingly certified voting system and a certified operational environment, the security concept evaluation effort is reduced to evaluating only a few remaining requirements not covered by those certificates. We therefore propose to combine these methodologies for the security concept based evaluation of VSPs. Thereby we enable the combined evaluation and make it usable for the VSP evaluation. We introduce the methodologies in the following sections. While the *IT-Grundschutz* methodology originates in Germany, we point out that the "*IT-Grundschutz* based on ISO27001" certification is internationally accepted, as is Common Criteria.

4.1 Common Criteria

The "Common Criteria for Information Technology Security Evaluation" (CC) is an international standard (ISO/IEC 15408) for computer security evaluation and certification[9]. CC focuses on the evaluation of IT products like hardware or software components. Besides the evaluation of concrete products, CC allows specifying generalized security requirements for a family of products in a 'Protection Profile' (PP). Manufactures thereby are enabled to develop corresponding products. An evaluation authority then evaluates and certifies the compliance of the product's security functionality with the PP. In 2008, the German Federal Office for Information Security certified and published the "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products" [*sic*] [VV08]. This PP specifies basic security requirements for online voting system software for non-political elections with low attack potential. The included requirements represent the essential foundation upon which voting systems for all election scenarios can build. It is an important step towards the certification of e-voting systems and is therefore planned to be mandatory for such systems in Germany. For our evaluation approach, the PP 'objectives' and 'assumptions' are relevant. The objectives specify the security goals which certified voting software is able to achieve.
In order to achieve these security objectives several assumptions are assumed to be realized, which cannot be achieved by the voting software. These assumptions must be satisfied by the operational environment. We show how PP-certified voting software can

[9] http://www.commoncriteriaportal.org/

facilitate the evaluation of a VSP. Our analysis revealed that many requirements included in the VSP's security concept can be fulfilled by such certified voting software and therefore do not need to be evaluated again in the VSP evaluation (see Section 4.3). Moreover we expanded the PP approach: since we incorporated the requirements from the catalog [Sc09b] into the security concept template (see Section 3.1), we especially included the assumptions towards the operational environment from the PP because these are contained in the catalog. Consequently a certified VSP realizes the secure operational environment assumed necessary in the PP to achieve the security objectives of the voting software. We discuss the applicability of the PP to the VSP scenario in Section 5. For further details on PP evaluation we refer to [VV08] and [VK07].

4.2 IT-Grundschutz/ISO27001

IT-Grundschutz (eng.: IT Basic Protection) provides a methodology to ensure and certify the security of complex 'information domains' which consist of infrastructural, organizational, personnel and technical components. *IT-Grundschutz* includes a comprehensive catalog of safeguards which can be implemented in order to satisfy protection requirements [G05]. The evaluation and certification methodology of *IT-Grundschutz* has been adapted to incorporate the methodology and the generic requirements on information security management systems from ISO27001 [Is08]. ISO27001 is an approved international standard that specifies requirements for the introduction, operation and improvement of information security management systems (ISMS) [KRS08]. It includes a sophisticated risk management methodology. ISO27001 is the first international standard for information security management that allows certification [G08a]. While ISO27001 specifies requirements, it only provides a very limited number of rather indefinite safeguards to fulfill those requirements. *IT-Grundschutz* can fill this gap by providing a multitude of concrete safeguards which can be used to satisfy the generic requirements from ISO27001. A synthesis of *IT-Grundschutz* and ISO27001 therefore seems plausible [KRS08]. Moreover, *IT-Grundschutz* includes predefined risk assessment to avoid a complex risk analysis at least in scenarios with normal protection levels. Concluding, the *IT-Grundschutz/ISO27001* approach facilitates implementation of the ISO27001 methodology by providing an immense set of safeguards and decreases efforts by reducing the need for costly risk analysis. Compared to classical risk analysis the *IT-Grundschutz* approach is more cost-effective and has been tested in practice for many years [G08a]. An *IT-Grundschutz/ISO27001* certification always includes an official ISO27001 certification, but, due to the additionally audited technical aspects, is more informative. The evaluation is performed by an external auditor certified by the German Federal Office for Information Security. In order to prove the achieved security level, *IT-Grundschutz* includes a certification methodology. There are three certification levels; the most comprehensive one is the 'ISO27001 certification based on *IT-Grundschutz,*' which incorporates the procedures and requirements of ISO27001 certification based on *IT-Grundschutz* safeguards.
The certification procedure comprises inspections of the reference documents, on-site inspection, and the generation of audit reports. For lower security level certification, *IT-Grundschutz* provides the less comprehensive and less costly 'entry level' (lowest level) and the 'continuation level' (intermediate level). The certification level is reflected

in according to safeguard categories. While the entry level certification only requires the implementation of safeguards of category A, the continuation level requires A and B. The ISO27001 certificate based on *IT-Grundschutz* requires all safeguards –A, B, and C– to be implemented. The additional 'Z' safeguards present supplements that can be used in case of higher security requirements.

4.2.1 *IT-Grundschutz* procedure

We describe the procedure an institution has to perform in order to secure its information domain according to the *IT-Grundschutz* methodology [G08a, G08b].
At first, the architecture, components, and processes of the information domain must be identified and documented. This is done in the *structure analysis*. Subsequently, the *determining of protection requirements* assesses the level of protection that is appropriate for the particular objects specified in the structure analysis. All objects are analyzed in regard to the potential damage that could result from an impairment of the protective goals of confidentiality, integrity or availability. Then the protection requirement for each object of the structural analysis is classified as "normal," "high," or "very high." Next, the *selection and adaptation of safeguards* must be accomplished. In this modeling process, the prior identified objects of the information domain are associated with respective *IT-Grundschutz* modules. The modules are comprised of generic aspects (e.g., personnel, contingency planning), infrastructure (e.g., server room), IT systems (e.g., laptop), networks (e.g., WLAN), and applications (e.g., database). Each module is associated with specific safeguards suitable to protect the module from typical threats. The safeguards are classified in the categories *A (entry level)*, *B (continuation level)*, *C (certificate)* and *Z (additional)* in accordance with the targeted certification level. All safeguards must be examined and adapted to the specific scenario to ensure the appropriate function. Adaptations must be documented. The result of the procedure is an *IT-Grundschutz* model for use as a test plan for an existing information domain or as a development plan for an information domain in planning. Next, the *basic security check* is performed to provide an overview over the existing security level by comparing current state and target state. Therefore applicability and current implementation status of each selected safeguard are checked. The basic security check reveals where additional steps have to taken in order to implement the *IT-Grundschutz* safeguards.

4.2.2 Handling special requirements

For efficiency reasons, *IT-Grundschutz* uses a two-stage approach. In the first stage, a normal protection level and a typical application scenario are assumed. Here, the *IT-Grundschutz* safeguards provide an adequate security level. These safeguards can be determined quickly and efficiently allow for increases in the security level of the information domain.
However, in some scenarios, especially in an electronic election scenario, some objects might require safeguards at a higher security level. Therefore *IT-Grundschutz* provides the *supplementary security analysis* in the second stage. At first, it is applied to objects whose protection requirement was classified "high" or "very high" in regard to at least one of the protective goals of confidentiality, integrity or availability in the preceding

analysis. Secondly, a supplementary security analysis is indicated, if a very specific object cannot be modeled appropriately due to the lack of respective *IT-Grundschutz* modules. At last, objects which can be modeled with *IT-Grundschutz* modules, but which are deployed in an untypical way or in an untypical environment shall undergo a supplementary security analysis as well. *IT-Grundschutz* provides several options on how to handle such special requirements. First, the before mentioned additional 'Z'-safeguards can be implemented to achieve a higher protection level. If not sufficient, an additional *risk analysis* needs to be performed. *IT-Grundschutz/ISO27001* recommends a risk analysis approach described in [G08c]. The intention is to determine threats to the information domain that are not considered sufficiently by the regular *IT-Grundschutz* safeguards and to find appropriate safeguards. We sketch the basic steps. For all target objects the basic *IT-Grundschutz* threats are listed. Additional threats are determined by analyzing the specific protection requirements and the operating scenario for the target objects. Threat probability and potential damage are assessed. The protection level of implemented safeguards is checked. Next, measures are determined to handle the risks– risks can be reduced by additional safeguards, risks can be avoided (e.g., by restructuring business processes), risks can be transferred (e.g., by insurance policies) and under certain circumstances (e.g., low threat probability upon extremely costly safeguards), risks can be accepted and therefore remain. Such residual risks must be assessed and documented. Next a second basic security check is performed to check whether the security level has been improved. At last, *IT-Grundschutz* allows for adaptation by adding new modules to describe threats and safeguards for specific components which are not included in the *IT-Grundschutz* catalog so far. We discuss the applicability of *IT-Grundschutz/ISO27001* to the VSP scenario in Section 5.

4.3 Incorporating Protection Profile and *IT-Grundschutz*

We demonstrate how the proposed PP and *IT-Grundschutz/ISO27001* evaluation methodologies can be incorporated in the security concept based VSP evaluation. In our security concept template we linked respective requirements to corresponding PP objectives, meaning that these requirements are covered by the referenced objectives and therefore satisfied by PP-certified voting software. Respectively, to each requirement that has to be satisfied by the operational environment, we linked suitable *IT-Grundschutz* safeguards. To this end, we assumed a generalized VSP architecture and components and mapped them to *IT-Grundschutz* modules. Our results thereby also show how utilizing PP-certified voting software and incorporating existing *IT-Grundschutz/ISO27001* can reduce costs and efforts in the VSP evaluation. Due to space limitations, we are restricted to presenting examples from our security concept template. In the first example a PP-certified voting system would significantly reduce the extent of evaluation. We list the applicable PP objectives that are achieved by a certified voting system. For their complete description, we refer to [VV08].

BALLOT CASTING

References: VSP act § 8, VSP ordinance § 3

PP objectives: O.Abort (b), O.OneVoterOneVote (b), O.Correction (c), O.Acknowledgement (d), O.Proof (e)

The VSP must ensure that the voters

a) are able to cast an invalid vote,

b) are able to abort the voting procedure without losing elective franchise,

c) are able to correct their vote any number of times until the final voting,

d) receive a confirmation for their vote,

e) are not enabled by the voting system to show their voting decision to others.

Besides a), all aspects are completely satisfied by a PP-certified voting system. The evaluation authority only needs to ensure that a) is fulfilled.

The next example shows how PP assumptions are integrated into the security concept template and how they can be satisfied by *IT-Grundschutz* safeguards [G05].

SYSTEM TIME

References: Operational environment requirements catalog [Sc09b]

PP assumption: A.SystemTime

IT-Grundschutz safeguards: B 3.3 Network components (S 4.227 Use of a local NTP server for time synchronization), B5 Security of applications (S 5.67 Use of a time stamp service)

The VSP must make the correct time and time stamps available to the voting system, conforming to the actual time. The required exactness is defined by the election host. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

In this case, the referenced *IT-Grundschutz* safeguards satisfy the assumption. *IT-Grundschutz* safeguards can also be used to satisfy many other requirements from the security concept; e.g., "Guarantee and maintenance of operation" (see Section 3.2) can be realized by implementing the modules "B 1.3 Contingency planning concept" and "B 1.8 Handling security incidents" [G05].
However, our findings revealed that *IT-Grundschutz* safeguards cannot cover all of the requirements in the template. For example, the voter registration or secure delivery of authentication means cannot be described appropriately by *IT-Grundschutz*. Availability or integrity safeguards from the *IT-Grundschutz* might not be sufficient for all election scenarios. We explain how to proceed in the next section.

4.4 Application guideline

To apply the security concept template we recommend that the VSP performs the *IT-Grundschutz* procedure described above in order to define the specific protection requirements of its system and to analyze to what extent the *IT-Grundschutz* safeguards referenced in the template fulfill these requirements. If certain requirements cannot be covered, a supplementary security analysis and, based on its result, a risk analysis should be performed. Remaining risks identified in this analysis have to be noted in the Section "Residual security risks" in the security concept (see Section 3.2).
If the VSP already has an *IT-Grundschutz* certificate which includes the respective safeguards noted in the template, the particular requirements are satisfied and do not need to be evaluated again. Otherwise the linked safeguards serve as a recommendation on how to satisfy the requirements. However, the operational environment is no plug-in component with exactly defined functional properties; *IT-Grundschutz* safeguards must always be adjusted to the specific local conditions. Therefore the applicability of an existing *IT-Grundschutz* certificate to the security concept and the election scenario always must be checked by the evaluation authority.
If PP-certified voting software is utilized, the VSP can skip the implementation of safeguards for the requirements which are already satisfied by the certified voting software. The evaluation authority only must evaluate whether the remaining requirements have been satisfied. This reduces the costs and effort of conducting a VSP evaluation. To optimize the evaluation, voting software manufacturers could include the fulfillment of these remaining requirements for the voting software from our template to their CC certification to prove not only PP-compliance, but additional 'VSP-suitability.'

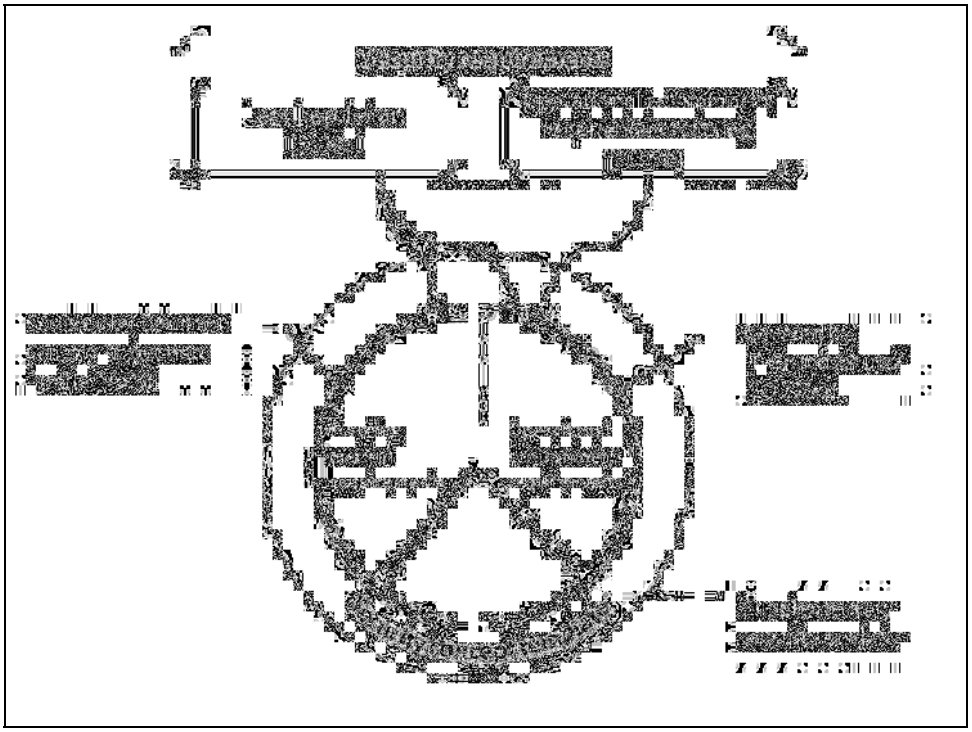


Figure 1: Application of evaluation methodologies

We illustrate our evaluation approach and the incorporation of the PP and *IT-Grundschutz/ISO27001* as well as the legal framework and the security concept template in Figure 1.

5 Discussion and Conclusion

We discuss the pros and cons of *IT-Grundschutz/ISO27001* and its applicability to the VSP scenario. Alternative certification methodologies like pure ISO27001 are mostly based on a general risk analysis approach. Threats and safeguards have to be determined from scratch. These are complex and costly tasks. In *IT-Grundschutz*, these steps are already integrated in every module of the *IT-Grundschutz* catalog. The large number of *IT-Grundschutz* safeguards simplifies implementation and can support the design process of VSPs. Hence, *IT-Grundschutz* evaluation is practicable. This supports the VSP approach. Basically, these safeguards ensure a normal security level for typical threats. This might not be sufficient for particular e-voting scenarios. However, *IT-Grundschutz* provides supplementary security analysis and risk analysis to adapt to special scenarios with higher protection requirements. Moreover new specific e-voting modules may be added to the *IT-Grundschutz* catalog. Consequently *IT-Grundschutz* seems applicable to the e-voting scenario and is a good choice for the certification of the operational environment of VSPs. Moreover, since many computer centers or similar IT

service providers already have *IT-Grundschutz* certificates, it facilitates their evaluation in case they want to provide electronic voting services as VSPs.
However, in the case of already existing *IT-Grundschutz/ISO27001* certification the implemented safeguards need to be checked during the VSP evaluation for their suitability in the e-voting scenario. The effort should be determined and assessed in practical tests. Furthermore *IT-Grundschutz* is mostly used in Germany. This might reduce acceptance abroad. However, since the legal framework for VSPs is built for the German context, this does not affect the integration of *IT-Grundschutz* in the security concept evaluation.
The applicability of the PP to the VSP scenario is obvious. To develop a state-of-the-art evaluation approach, we need to incorporate this important evaluation concept for voting software. Admittedly, the PP is intended only for non-political election scenarios with low attack potential. However, it represents a foundation of requirements all other election scenarios build upon. Furthermore, since the legal framework for VSPs includes non-political elections as well, the PP perfectly fits into the VSP scenario. Regarding the incorporation of the PP into the VSP evaluation, this is an improvement on both sides; from the VSP perspective, using PP-certified voting software significantly facilitates the VSP evaluation. From the PP perspective, our VSP evaluation approach closes the gap of the PP evaluation because now the VSP is certified to achieve all open PP assumptions towards the operational environment. Thereby an overall evaluation is achieved. A VSP certified according to the security concept template complies with the legal framework, it represents the required operational environment for voting systems certified according to the PP, and it achieves the state-of-the-art in operational environment security as demanded in [Sc09b]. We point out that our combined evaluation approach of voting system and operational environment might be adapted to other e-voting scenarios outside the VSP context. However the existing legal framework, the security concept and the centralized design make the VSP scenario an ideal basis.
In this paper we presented a security concept template for VSPs and a corresponding evaluation methodology. By incorporating existing evaluation methodologies into the security concept evaluation, we presented a realistic approach which reduces the costs and effort of an evaluation. Concluding our work helps to enable the VSP concept and improves e-voting evaluation by combining the evaluation of voting systems and operational environment.

Bibliography

[Co04] Council of Europe. 2004. Legal, operational and technical standards for e-voting, Recommendation Rec(2004)11, Council of Europe Publishing, Strasbourg.

[G01] German Ordinance on Electronic Signatures (Signaturverordnung). 2001. http://bundesrecht.juris.de/sigv_2001/index.html/.

[G05] German Federal Office for Information Security. IT–Grundschutz Catalogues. 2005. http://www.bsi.de/english/gshb/download/it-grundschutz-kataloge_2005_pdf_en.zip/.

[G08a] German Federal Office for Information Security. 2008. BSI-Standard 100-1 Information Security Management Systems (ISMS), Version 1.5.

[G08b] German Federal Office for Information Security. 2008. BSI-Standard 100-2 IT-Grundschutz Methodology, Version 2.0.

[G08c] German Federal Office for Information Security. 2008. BSI-Standard 100-3 Risk analysis based on IT-Grundschutz, Version 2.5.

[G08d] German Federal Office for Information Security. 2008. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits.

[Ha92] Hammer, V., Pordesch, U., Roßnagel, A.:. 1992. KORA - eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme, Arbeitspapier 100. provet, Darmstadt.

[Ha94] Hammer, V., Pordesch, U., Roßnagel, A., Schneider, M.J. 1994. Vorlaufende Gestaltung von Telekooperationstechnik - am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft, GMD-Studien Nr. 235. Sankt Augustin.

[Id00] Idecke-Lux. 2000. Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz. Nomos. Baden-Baden.

[Is08] ISO/IEC 27001:2005 Information Technology - Security Techniques - Information Security Management Systems Requirements Specification, ISO/IEC JTC1/SC27, 2008.

[KRS08] Kersten, H., Reuter, J., Schröder, K.-W. 2008. IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Vieweg, Wiesbaden.

[La08] Langer, L., Schmidt, A., Buchmann, J. 2008. Secure and Practical Online Elections via Voting Service Provider. In *Proceedings of ICEG 2008*, 255-262. ACI.

[RJ07] Reinhard, K.; Jung, W. 2007. Compliance of POLYAS with the BSI Protection Profile–Basic Requirements for Remote Electronic Voting Systems. In*VOTE-ID*, Lecture Notes in Computer Science vol. 4896, ed. A. Alkassar and M. Volkamer, 62–75. Springer.

[Re07] Republic and Canton of Geneva State Chancellery. Report by the Geneva government to the Geneva parliament on the internet voting project. 2007. http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf/.

[Sc09a] Schmidt, A., Heinson, D., Langer, L., Opitz-Talidou, Z., Richter, P., Volkamer, M., Buchmann, J. 2009. Developing a legal framework for remote electronic voting. In *Proceedings of VOTE-ID 2009 Second international conference on E-voting and Identity, Luxembourg, LNCS 5767*, 92-105. Springer.

[Sc09b] Schmidt, A., Volkamer, M., Langer, L., Buchmann, J. 2009. Towards the impact of the operational environment on the security of e-voting. In *Proceedings of INFORMATIK 2009, LNI 154*, 1814-1826. GI.

[Tr09] Tranchard, S. 2009. The State of Geneva designs a secure Internet voting system. In *ISO Focus* 6:38-39.

[VKG07] Volkamer, M., Krimmer, R., Grimm, R. 2007. Independent Audits of Remote Electronic Voting - Developing a Common Criteria Protection Profile. In *Proceedings of Elektronische Demokratie in Österreich - EDEM '07*, 115-126. Vienna: OCG Verlag.

[VV08] Volkamer, M., Vogt, R. 2008. Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte. Common Criteria Protection Profile BSI-PP-0037. https://www.bsi.bund.de/cln_156/ContentBSI/Themen/ZertifizierungundAkkreditierung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0037/.

[WVM07] Weldemariam, K., Villafiorita, A., Mattioli, A. 2007. Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach. In *Proceedings of the F*irst C*onference on E-Voting and Identity (VOTE-ID), LNCS 4896.*

Session 5: End to End Verfifiability and Protocol Improvements

Verifiability in Electronic Voting
Explanations for Non Security Experts

Rojan Gharadaghy and Melanie Volkamer

CASED—Center for Advanced Security Research Darmstadt
Technische Universität Darmstadt
Mornewegstraße 32, 64293 Darmstadt
Germany
{rojan.gharadaghy, melanie.volkamer}@cased.de

Abstract: Scientists have requested verifiable electronic voting schemes for many years. These schemes offer individual and universal verifiability by applying and combining complex cryptographic primitives and protocols. Electronic voting systems in use provide less or even no verifiability. Thus election authorities and voters need to trust the provider and developer of the voting system regarding the integrity of the election. Due to arising critiques and the voting computer decision of the Federal Constitutional Court in Germany, the future electronic voting systems will probably need to implement verifiability. Therefore, this paper presents an overview and analysis of approaches to implement verifiability. We mainly address non-security experts like the average election authority and the average voter. Thus, the paper supports election authorities in their decision making process for a verifiable electronic voting system and the voter in making use of the verifiability.

1 Introduction

Electronic voting and in particular remote electronic voting offers many advantages compared to traditional paper based elections: like lower costs, faster tallying, improved accessibility and flexibility to the voter, greater accuracy of the result, lesser unintended invalid votes, and lower risk of human errors. However, an election can only profit from these advantages if the electronic voting system used ensures the four election principles of an equal, universal, secret, and free election. From an IT security point of view, these principles mainly mean that an electronic voting system has to ensure the secrecy of the vote and the integrity of the election result. Both must not be vulnerable to an outside attacker (i.e., hackers) nor to an inside attacker (i.e., developers, server/system hosts and administrators, and voters). Electronic voting systems used so far (e.g., in Estonia, the Netherlands, Austria, and Germany) have been evaluated by security experts. These evaluations mainly intended to check the system's robustness against outside threats while the election authorities and the voters have to trust that the developer and provider of the electronic voting system are not corrupt nor do they violate the election principles.

The problem is that once these systems are installed and the election is started, it is very difficult, if not impossible, to check whether the evaluated system and only this system is running[1] (for the entire voting period). As malicious providers could effect the system in several ways, (e.g., change the voting software undetected, log additional data, implement backdoors, change entries in databases in order to modify the election result or break the secrecy of the vote) verifiability mechanisms are necessary to run secure and trustworthy electronic elections. With these mechanisms voters and the public are able to audit the integrity of the election and thus the election result is ensured. Thus one can trust the provider, but the trust can also be audited. Note, even in traditional elections, trust in the people running the election (e.g., poll workers in the polling station) is not unlimited because observation in polling stations and other relevant places (e.g., central tallying) are allowed–sometimes required (compare [BWahlG, NRWO]).

Due to the fact that (a) the trustworthiness of a system rises if the system implements verifiability in addition to a security evaluation [Vo09]; (b) critiques have increased against the so-called black box voting systems; and (c) the German Federal Constitutional Court demanded verifiability for (electronic) voting in its voting computer decision [BFG09], the future electronic voting systems will probably need to implement verifiability mechanisms. The decision for a particular verifiability electronic voting system is made by the election authority, and the verifiability mechanisms themselves need to be applied by voters and observers. The problem is that verifiability approaches are based on complex cryptographic primitives and protocols. These approaches are only understandable to those with a background in cryptography. This is not the case for the average election authority or voter. Therefore, this paper presents an overview and analysis of existing technologies to implement verifiability from a non-security expert perspective. A couple of "important to know" statements have been identified and are labeled correspondingly. We point out the advantages and disadvantages of different approaches. The paper supports election authorities in their decision making process for a verifiable electronic voting system. It further helps voters to understand the advantages and boundaries of verifiable voting systems as well as to apply verifiability mechanisms in a future electronic election.

The remaining part of this paper is structured as follows: First, in Section 2, we give a short introduction on verifiability in general. The focus of Section 3 is individual verifiability and how this can be realized, while Section 4 concentrates on different aspects of and different approaches for universal verifiability. Section 5 concludes this paper.

2 Verifiability

In the electronic voting literature, verifiability addresses the security requirement of the integrity of the election result. First of all, this means that it is possible for the voter to audit that his/her vote has been properly created (in general encrypted), stored, and

[1] Trusted computing techniques could help here, but would require special hardware and software at the voter's PC. Therefore, these approaches cannot be applied to voting.

tallied (the so-called *individual verifiability*). Further, this means that everyone can audit the fact that only votes from eligible voters are stored in a ballot box, and that all stored votes are properly tallied (the so-called *universal verifiability*[2]) [La09]. Systems providing both forms are called End-to-End (E2E) verifiable [Be09].

> **(Important to know 1)** Even with a verifiable electronic voting system, it is still possible for malicious providers and system developers to manipulate the (integrity of the) election result, but due to the verifiability, it will be detected. Thus it is not necessary anymore to trust them (regarding the integrity of the election result[3]).
>
> **(Important to know 2)** It is not required that each voter makes use of the individual verifiability or that all voters, candidates, parties, and observers make use of the universal verifiability. As a malicious provider does not know who verifies his/her vote and who does not, the provider cannot manipulate single votes without being detected with a very high probability. Regarding universal verifiability, it would even be sufficient if one trustworthy entity verifies the tallying.

Implementing verifiability in general would be easy. For instance a doodle[4] poll is perfect verifiable as everyone can go to the doodle web page after having cast a vote and verify that the vote next to his/her name has not been altered. Further he/she can verify that the result is correct by tallying each vote next to the voters' names (if the corresponding person is eligible to vote). But, if an electronic voting system needs to ensure the secrecy of the vote (which a doodle poll does not), it is necessary to apply and combine complex cryptographic primitives and protocols[5].

> **(Important to know 3)** Even with these cryptographic techniques, it is not possible to provide unconditional[6] verifiability and unconditional secrecy of the vote at the same time**.** Protocols ensure either unconditional verifiability and computational[7] secrecy of the vote or vice versa (compare [Ad08]).

Bulletin Boards (BB) have been invented in order to implement verifiability in electronic voting (for both remote electronic voting and electronic voting devices). BBs are public broadcast channels like web pages in the Internet, which have special properties: Data is published only by authorized parties and, once published, cannot be deleted or modified anymore. Such a Bulletin Board can be accessed (with read access) by everyone for verifiability purposes—including the voter and the election authority. The Bulletin

---

[2] Other terms are public auditable or open audit [La09].

[3] Ideally, an electronic voting system would also provide the possibility to verify that the secrecy of the vote and maybe also other requirements are ensured (see [Vo09]). This is not covered in this paper.

[4] http://www.doodle.com/

[5] For electronic voting devices, it is also possible to realize verifiability without cryptography by using voter verifiable paper audit trails, printed by the devices and stored in a traditional ballot box. As the authors do not see a real benefit in these systems, this is not further addressed here.

[6] Unconditional means perfectly verifiable; even very powerful attackers cannot violate the integrity of the election result without been detected.

[7] Computational means that it depends on the solvability of a mathematical problem, which is classified as hard to solve. However, very powerful attacks would be able to break it. In general these problems are hard to solve today, but this might change in future.

Board contains and displays at least a list of cast votes (in encrypted form) together with voters' IDs or pseudonyms, and a couple of proofs used for verifiability (see Figure 1). The concrete content depends on the implemented verifiability approach. With the help of the Bulletin Board, verifiability can be done from any place at any time over the Internet—independent of whether the vote casting took place at an electronic voting system or over the Internet. Thus verifiability becomes possible for everyone not only those observing the process in the polling station. This is a main advantage compared to traditional paper based elections.

(Important to know 4) Bulletin Boards are a necessary concept to implement verifiability in electronic voting.

Verifiability can be achieved either "by hand" (by those who understand the underlying cryptography and are able to program their own verifiability) or by verifiability tools provided by independent institutes (for average voters and election authorities to run the verifiability). These could be downloadable or accessible through corresponding web pages. Moreover, the voter could also ask institutes like a university to run the verifiability on his/her behalf.

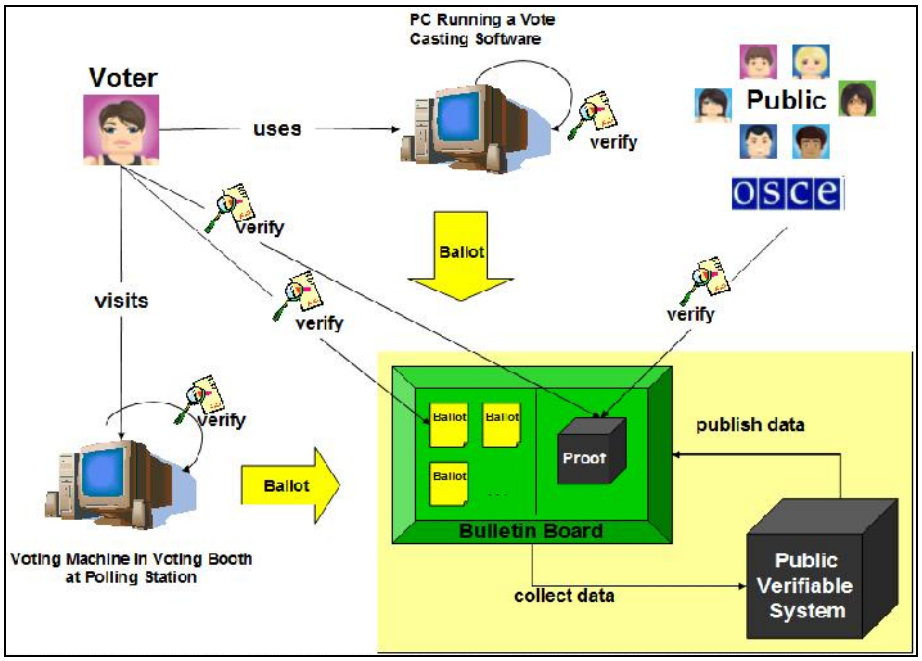


Figure 1: Overview on verifiability in electronic voting

(Important to know 5) Verifiability tools/software needs to be available from independent institutes so that the voter can choose the one he/she trusts.

2.1 Individual verifiability

Individual verifiability addresses the voter. The goal of individual verifiability is that the voter can verify that

(a) his/her vote is properly encrypted (during vote casting), i.e., if he/she chooses candidate *A* then candidate *A* is also encrypted and not candidate *B* [cast as intended];
(b) his/her encrypted vote is sent and stored unaltered at the Bulletin Board (after vote casting), i.e. if candidate *A* has been encrypted to $enc(vote_A)$ then $enc(vote_A)$ must appear on the Bulletin Board next to the voter's ID/pseudonym and not $enc(vote_B)$ [stored as cast];
(c) his/her encrypted vote is properly included in the election result (after tallying), i.e., in general properly decrypted and properly added to the other decrypted votes [tallied as stored].

Part (c) is only covered indirectly by universal verifiability. The idea is that if it is verifiable for all encrypted votes on the BB that they are properly included in the tally then this also holds for a particular vote [La09].

(Important to know 4) Individual verifiability ensures that the vote is cast as intended and stored (on the BB) as cast (part (a) and (b)).

(Important to know 5) Due to part (b), there exist a link between the voter/ pseudonym and his/her encrypted vote on the Bulletin Board. Consequently, once the encryption scheme is broken the secrecy of the vote is violated, if there is a link between voter and encrypted vote.

2.2 Main idea and first approach

Implementing individual verifiability can be realized relatively easy in the following way: votes are encrypted probabilistic, that is, votes are concatenated with a random number and then encrypted[8] *enc(vote#[9]R)*[10]. In general, knowing the values *vote* and *R* means that it is possible to "decrypt" this term without the knowledge of the decryption key: just by encrypting the value *vote#R* again and comparing the output with the encrypted term *enc(vote#R)*. Based on this, the individual verifiability can be implemented in the following way:

- The voter uses an individual verifiability tool.
- This tool gets as input from the voting application the encrypted vote *enc(vote#R)* and the random value *R* used for the encryption plus from the voter the value *vote*.
- This tool audits whether *the vote has been encrypted properly*.

[8] Public-key encryption is used, which means that a message is encrypted with the public key of the receiver, and the encrypted message can only be decrypted with the corresponding secret key, which is only known by the receiver.
[9] The symbol # is used for concatenations.
[10] Without this value *R* the encryption does not really protect the confidentiality of the vote as an attack could easily encrypts all possible votes and compares the output with *enc(vote)*.

- If this is the case, the encrypted vote is transferred to the Bulletin Board and stored.
- In order to later verify that the vote is properly stored on the BB, the random number is stored on the voter's PC.
- After having completed the vote casting, a voter can use the individual verifiability tool again to verify whether *his/her encrypted vote is properly stored* on the Bulletin Board.
- This time, the tool takes as input the stored random value *R* and from the voter, his/her choice and some personal information to identify the voter's entry on the BB.
- With this information the tool computes *enc(vote#R)* and verifies whether this value is on the Bulletin Board. Note, both verifiability checks can be repeated with arbitrary individual verifiability tools.

The described approach provides unconditional individual verifiability. But, it violates the secrecy of the vote because it is not receipt-free[11]. A voter could use his/her knowledge of the randomness *R* as a receipt to prove to himself/herself that he/she cast his/her vote.

2.3 Advanced approach

In order to avoid such a receipt and thus be receipt-free, the above described mechanism for individual verifiability needs to be modified in the following way (see, e.g., [Ad09, Ad08]):

- Here, after the voting application has encrypted the vote, the voter needs to decide whether he/she wants to verify that the *vote has been properly encrypted* or whether the voter wants to cast the vote (which means the encrypted vote is sent to and stored on the Bulletin Board while the encrypted vote is stored on the voter's PC[12]).
- Only, if the voter decides to verify the encrypted vote, the random value *R* is revealed as input for the individual verifiability tool.
- If the voter decides to cast the vote, the value *R* is not revealed to ensure receipt-freeness.
- In this approach, the *second part* of the individual verifiability works as follows: The voter uses the individual verifiability tool again.
- This tool takes as input the stored encrypted vote and from the voter some personal information to identify his/her entry on the Bulletin Board. It verifies whether the encrypted vote appears on the BB.

The consequences for the individual verifiability in this approach are the following:

- [cast as intended] The voter cannot verify whether the cast encrypted vote contains his/her candidate choice. After having successfully verified a couple of (test) votes,

[11] Receipt-free means that the voter does not get a receipt to prove which candidate he/she chose.
[12] In this approach, the randomness *R* is neither leaked to the voter nor stored on his/her PC.

the voter has good evidence that his/her cast vote is also properly encrypted. The idea is that the voting application does not know how the voter will decide and thus does not know when (in case it would be malicious) to encrypt a different vote.

- [stored as cast] While in the previously described approach the voter could verify that the encrypted vote on the BB contains his/her candidate choice, in this approach he can only check whether the stored encrypted vote is properly stored on the Bulletin Board. However in combination with the evidence from the first part of the individual verifiability (cast/encrypted as intended), this is acceptable.

(Important to know 6) In order to verify that his/her vote is cast, the voter needs to verify his vote twice: once during vote casting and once after vote casting/after tallying. Thus there are two additional steps compared to black box voting systems if the voter wants to apply individual verifiability.

(Important to know 7) In order to provide receipt-freeness, a voter gets only evidence with high probability but no formal proof for the individual verifiability because the vote he/she finally cast cannot be verified, but only arbitrary votes before.

3 Universal verifiability

Universal verifiability is more complex than individual verifiability. At least two comparable (cryptographic) approaches exist. This section is structured into the following subsections: In the subsection 3.1, the main idea is proposed as well as its high level implementation and challenges in realizing it. The two main cryptographic approaches (one based on so called MIX networks and the other one based on the homomorphic property of encryption schemes) are introduced and explained in subsection 3.2.

3.1 Idea and Challenges

After the voting period for each voter who cast a vote, a corresponding encrypted vote is stored and published on the Bulletin Board[13].

(Important to know 8) The universal verifiability needs to ensure that all of these stored votes are properly tallied[14]. This usually also includes that the decryption is done properly.

The easiest way to implement universal verifiability would be to decrypt each vote on the Bulletin Board and publish all decrypted votes and the decryption/secret key. These data enable everyone to tally the votes him/herself or by using a universal verifiability tool and to verify that the votes are properly decrypted with the decryption/secret key. However, this would violate, in the worst case, the secrecy of the vote (if the encrypted

[13] Each encrypted vote can be unambiguously linked to a voter or his/her pseudonym. This is necessary to enable the individual verifiability.

[14] [Ry09] also recommends verifying that all votes are cast by eligible voters. We agree that this is necessary. However, due to time and space constraints this is not covered by universal verifiability in this paper.

votes are linked to the voters ID), and in any case, the system would not be receipt-free. Thus the Bulletin Board would contain either the information: *voter ID – encrypted vote – decrypted vote* or at least *voter's pseudonym – encrypted vote – decrypted vote.*
Obviously, it is challenging to compute the election result without violating the secrecy of the vote and being receipt-free. Therefore, one of the following two cryptographic techniques is applied to meet this challenge with corresponding cryptographic protocols (compare to [Sc08, Sm05])[15]:

- Cryptographers have developed encryptions schemes (so called homomorphic schemes), which allow the encrypted sum of all encrypted votes to be computed. Decrypting this sum is equal to the sum of all decrypted votes, i.e., *dec**(**enc(vote1) + enc(vote2) + ... + enc(voten))** = dec**(**enc(vote1))** + dec**(**enc(vote2))** + ... + dec**(**enc(voten))***. The main advantage of this approach is that it is not necessary to decrypt single votes. The decryption/secret key is only used once to decrypt the result. Therefore, the secrecy of the vote is ensured at the same time (see also Figure 2 and compare to Section 3.2.1).
- The second approach is based on the idea that the encrypted votes are first anonymized and then decrypted. To do so, the encrypted votes are first of all separated from the voter's ID/pseudonym. This set of encrypted votes is then anonymized by using a so called MIX net (compare to [Ch81]). A MIX net contains several nodes (so called MIX nodes which are general servers, running a particular software) while each MIX node takes as input the set of encrypted votes, shuffles this set and outputs a list of anonymized encrypted votes. This is done by each MIX node. Finally after shuffling the votes several times, the anonymized votes are decrypted and tallied. Several MIX nodes are used to increase the trust in the secrecy of the vote; although it is enough if one MIX node is trustworthy and anonymized the set of encrypted votes by shuffling the encrypted votes (see also Figure 3 and compare to Section 3.2.2).

(Important to know 9) Two different approaches are distinguished for a tallying procedure that ensures the secrecy of the vote: (a) Either only the encrypted sum is decrypted (while single votes are never decrypted) or (b) the encrypted votes are anonymized by randomized shuffling and only the anonymized votes are decrypted.

A *universal* verifiability tallying procedure needs to ensure the secrecy of the vote while providing proofs of the election result's integrity, that is, proving that the tallying procedures ran appropriately. Thus proofs need to be created during the tallying. This makes the tallying more complex and also a little bit slower. Although it becomes more complex and involves more entities in the tallying, the robustness of the tallying needs to be ensured, i.e., running the tallying should not relay on single entities. No single (malicious) entity should be able to block the computation of the election result, e.g., by claiming to having lost the decryption/secret key.

[15] Actually in [Sm05], two more approaches are named. However, these are not very popular and thus not included in this paper. They are "heterodox schemes" and "schemes based on secret sharing among several mutually distrustful election authorities."

(Important to know 10) A universal verifiability approach needs to ensure the secrecy of the vote and needs to be robust while providing proofs of the election result's integrity.

In order to get a universal verifiable voting scheme, it is necessary to extend the above described approaches (homomorphic encryption function / MIX nets) with corresponding proofs.

3.2 Two main approaches

The main idea of universal verifiability is to ensure that the tallying is done properly. Thus for both approaches, we explain what can go wrong in terms of where manipulations of the election results' integrity can occur and which techniques can be used to provide universal verifiability, i.e., make such manipulations detectable.

3.2.1 Approach based on homomorphic encryption

In a universal verifiably scheme based on homomorphic encryption, the following two manipulations must be detectable with corresponding proofs:

- The system provides an arbitrary result as output for the decryption of the encrypted sum.
- The key holder(s) get the wrong decryption/secret key. This wrong key is used for decryption. The corresponding output is not equal to the sum of decrypted votes. Thus the integrity of the election result is not ensured.

Further, the robustness of the tallying procedure should not depend on the one key holder of the decryption/secret key.

To improve the robustness, the secret key is shared by several authorities with a so-called secret sharing scheme [Sh79]. This can be done in a way that k out of n authorities are already able to decrypt a message (in this scheme the encrypted sum of all votes). Thus if some authorities lose their key shares, the result can still be determined. To overcome the problem of the key holders receiving the wrong keys, so called verifiable secret sharing schemes are applied [Ch85]. Here it can be proven that the shares are properly distributed. Cryptographers also developed methods to prove that a message was properly decrypted without revealing the secret key (this is necessary to ensure the secrecy of the vote). One possibility of proving the correctness of a decryption is to use the Chaum-Pedersen protocol [CP92]. Using all three techniques the tallying is universal verifiable and at the same time proofs are provided in two situations: one after the key distribution and the other one with the decryption of the election result. Correspondingly, in both situations the proofs need to be verified. Moreover, it needs to be verified that the encrypted sum has been calculated correctly. An overview of the universal verifiability approach based on homomorphic encryption is shown in Figure 2.

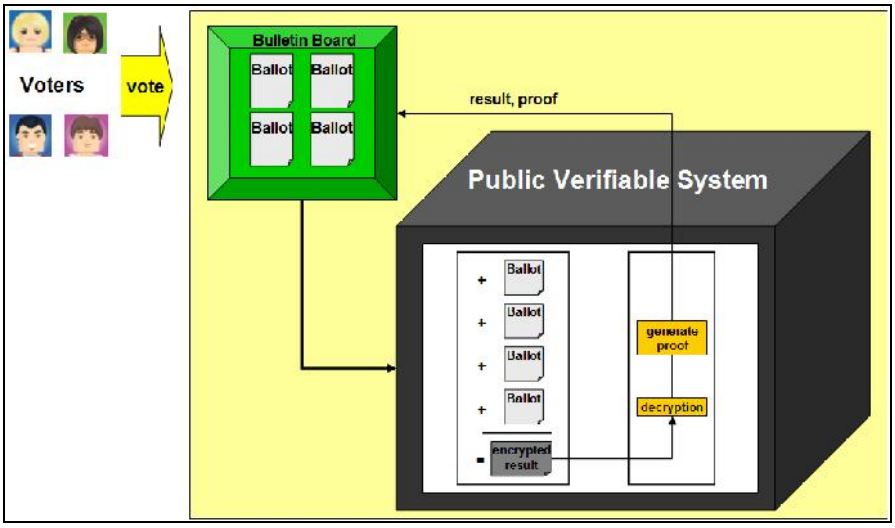


Figure 2: Universal verifiability based on homomorphic encryption

3.2.2 MIX-based approach

In a universal verifiably scheme based on homomorphic encryption, the following three manipulations must be detectable:

- The output of a MIX node does not correspond to the shuffled input because encrypted votes have been modified. (1)
- The component finally decrypting the votes provides an arbitrary result for the decryption of each vote. (2)
- The key holder(s) got the wrong decryption/secret key. This key is used to decrypt votes. The corresponding output is not equal to the cast vote. (3)

Further, the robustness of the tallying procedure should not depend on the one key holder of the decryption/secret key and not on each MIX node. To increase the robustness of the MIX net so called re-encryption MIX nets are used. This means that arbitrary MIX nodes can fail and arbitrary new MIX nodes can be added to increase the trust in the secrecy of the vote. To increase the robustness with respect to the key holder and to ensure (2) and (3), the same techniques as for the homomorphic approach are used (namely: verifiable secret sharing and a proof of correct decryption). In addition, it needs to be ensured that each MIX node cannot manipulate the election result by altering the votes from the input to the output. To do so, cryptographers either use Zero Knowledge Proofs or Randomized Partial Checking [JJR02]. The first provides a real proof while the second approach only provides high evidence. However, the second approach is much more efficient than the first one.

Using all these techniques, the tallying is universal verifiable, and proofs/evidences are provided in three situations: (similar to the homomorphic approach) one after the key distribution and the other one with the decryption of the election result; plus the proofs/evidence provided by each MIX node. Correspondingly, in all three situations the proofs/evidence needs to be verified. The universal verifiability approach based on MIX nets is shown in Figure 3.

(Important to know 11) While there is less effort involved in the tallying and verifiability of homomorphic schemes, not all election schemes can be run using this approach because for some schemes (e.g., with write-in ballots) a corresponding homomorphic encryption scheme does not exist.

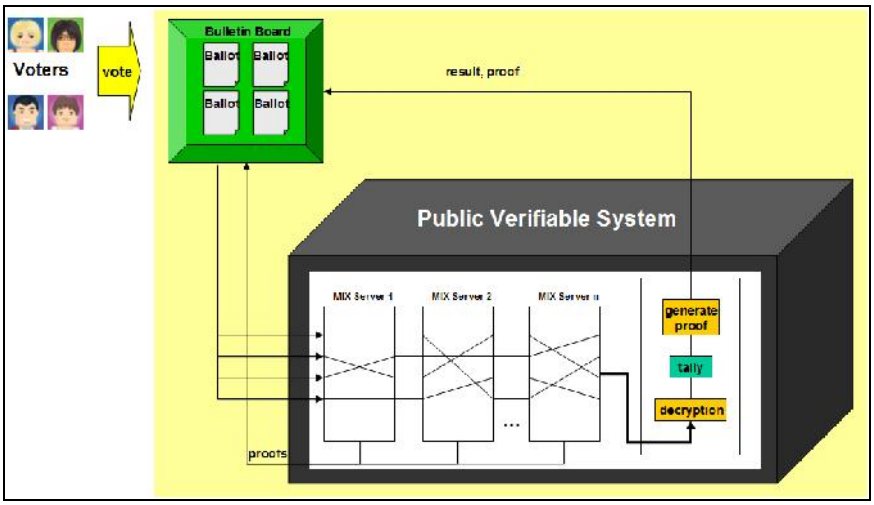


Figure 3: Universal verifiability based on a verifiable MIX net

4 Conclusion

Verifiability (both universal and individual) in electronic voting is becoming more and more important. After having discussed these techniques for years in the research community, this now needs to be implemented in future electronic voting schemes. Due to the fact that these techniques need to ensure the secrecy of the votes, the approaches are rather complicated and suffer from different constraints. The most important one is the theorem that an electronic voting system can either ensure unconditional secrecy or unconditional verifiability. Further, the election authority has to decide which verifiability approach they are in favor of.

This paper explains the different approaches from a high level perspective to also enable non-security experts to decide which technique to use and what its advantages and disadvantages are. Further, this paper addresses voters to help them understand what the advantages of verifiable voting schemes are and how to use them.

However, even if this paper helps to understand verifiability in the context of electronic voting, in order to use these techniques for legally binding elections, there are two open issues: First of all, the user friendliness has to be increased to enable average voters to use the verifiability mechanisms. Second, it is necessary to develop technical and/or organizational mechanisms and policies to handle those cases in which the result of any verifiability is negative.

Bibliography

[Ad08] Adida, B. 2008. Web-based open audit voting. In *Proceedings of the 17th symposium on security,* pp. 335–348. Berkeley, CA, USA: USENIX Association.

[Ad09] Adida, B. et al. 2009. Electing a niversity President Using Open-Audit voting: analysis of real-world use of Helios. In *EVT'09. Proceedings of electronic voting technology workshop.* USENIX Association.

[Be09] Benaloh, J. 2006. Simple verifiable elections. In *EVT'06. Proceedings of the USENIX/accurate electronic voting technology workshop*. Berkeley CA, USA: USENIX Association.

[Ch81] Chaum, D.. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. In *Communications of the ACM 24, February, Nr. 2*, pp. 84–90..

[CP92] Chaum, D. and T. P. Pedersen. 1992. Wallet databases with observers. In *CRYPTO, volume 740 of LNCS*, 89–105. Springer.

[Ch85] Chor, B. et al. 1985. Verifiable secret sharing and achieving simultaneity in the presence of faults. *In FOCS85,* pp. 383-395.

[BWahlG] *Bundeswahlgesetz in der Fassung der Bekanntmachung vom 23. July 1993 (BGBl. I S. 1288, 1594), last change 17. March 2008 (BGBl. I S. 394).*

[NRWO] *Bundesgesetz über die Wahl des Nationalrates (Nationalrats-Wahlordnung 1992 – NRWO) BGBl. Nr. 471 idF BGBl. I Nr. 28/2007.*

[BFG09] *BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1–163), Urteil des Zweiten Senats*. http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html/.

[JJR02] Jakobsson, M., A. Jueles, and R. L.Rivest. 2002. Making mix nets robust for electronic voting by randomized partial checking. In *Proceedings of the 11th symposium on security,* pp. 339–353. Berkeley, CA, USA: USENIX Association.

[La09] Langer, L. et al. Unpublished. Towards a framework on the security requirements for electronic voting protocols. In *Post Proceedings of RE-Vote09*.

[Ry09] Ryan. M. 2009. *Verifying electronic voting protocols in the applied pi calculus*. Slides presented at the 3rd workshop on security and electronic voting (VETO 09). http://www-veto2009.imag.fr/Material/Mark Ryan.pdf/.

[Sc99] Schoenmakers, B. 1999. *A simple publicly verifiable secret sharing scheme and its application to electronic voting*. Technical report. Eindhoven, NL: Department of Mathematics and Computing Science, Eindhoven University of Technology.

[Sc08] Schoenmakers, B. 2008. Voting schemes. Draft book chapter. To appear in *Algorithms and theory of computation handbook, http://www.win.tue.nl/~berry/ papers/ChVotingSchemesJuly2008.pdf*

[Sh79] Shamir, A. 1979. How to share a secret. *Communications of the ACM* 22 (11): 612–613.

[Sm05] Smith, W. D. 2005. Cryptography meets voting. http://www.math.temple.edu/ ~wds/homepage/cryptovot.pdf

[Vo09] Volkamer, M. et al. 2009. Elektronische Wahlen. Verifizierung vs. Zertifizierung. *Proceedings of INFORMATIK 2009, volume 154 of LNI*, 1827-1836. Bonn, Germany: Gesellschaft für Informatik.

Verification Systems for Electronic Voting: A Survey

Jordi Pujol-Ahulló, Roger Jardí-Cedó, and Jordi Castellà-Roca

Departament d'Enginyeria Informàtica i Matemàtiques
UNESCO Chair in Data Privacy
Universitat Rovira i Virgili
Av. Països Catalans 26
E-43007 Tarragona, Spain
{firstname.lastname}@urv.cat

Abstract: Voting is an important part of the democratic process. The electorate makes a decision or expresses an opinion that is accepted for everyone. Some parts could be interested in the election results deviation without anyone else noticing it. However, ensuring that the whole voting process is performed correctly and according to current rules and law is, then, even more important. We present in this work a review of existing verification systems for electronic voting systems, from both academia and the commercial world. To do so, we realize a fair comparison against a set of representative voting verification systems, by using an evaluation framework. We define this framework to be composed of several properties and covering important system areas, ranging from the user interaction to security issues. We then model the natural evolution of verifiability issues on electronic voting systems, which are influenced by restrictions on current laws and by technological advances.

1 Introduction

From the birth of democracy in Athens in sixth century BC and the first form of electoral laws, electoral systems have been designed and developed according to country particularities in democratic governments worldwide.

An election process consists of choosing a person or party, namely *candidate*, to represent all members of the community (e.g., a company, a state, or a country). For a candidate, winning an election represents a big responsibility, but it is also very attractive in many ways for other reasons (e.g., funds, ability to change existing rules and laws). Therefore, synergies could appear to deviate from election results to have a certain candidate (not) win.

However, it is a difficult task to check whether the election results correspond to the voters' preferences, since *votes are commonly private and anonymous*. That is, if voter Alice votes for candidate A, any another person must not know or extract Alice's preferences from the election process and results.

In other words, *elections must be verifiable*, even though voters' preferences are linked in no way to them. Therefore, *verifiability* comes to light as the most important election property to provide *trustfulness* to the election results to both candidates and voters.

Verifying that election results correspond to voters' preferences depends on the voting system. From a location viewpoint, most of the existing systems are based on *poll sites*, where voters go to specific places to vote. Remote voting systems (such as mail voting or lastly internet voting systems) are also an alternative.

From a ballot perspective, traditional voting systems use ballots in paper format. They were firstly introduced in the state of Victoria, Australia, in 1856 [Be10]. Paper ballots contain all the necessary information to vote for a specific candidate, in a human-readable format. Thus in the vote counting or *tally*, any person can verify whether the ballot is correct and, if so, to which candidate it is related to. However, the main drawbacks of traditional voting systems are that all operations are manual, as well as their high economic and logistic costs. In addition, the tally process where votes are counted can turn into a long procedure susceptible to human errors, especially when the voting system is complex.

More modern voting solutions incorporate electronic devices to mainly accelerate the tally process and overcome the problems induced by human errors, and also increment accessibility for disabled and illiterate voters. First initiatives appeared in 1964 in some states of the USA, which used punchcards and computer tally machines [Be10]. These kinds of solutions can use different technologies, ranging from punchcards, optical scanners (to scan ballots), to cryptographic techniques. Electronic voting (e-voting) systems thus pose other kinds of challenges to election *verifiability*, whilst at the same time ensuring voter privacy and anonymity.

To put all of this in words, we can differentiate three different types of *verifications*: *individual*, *universal* and *end-to-end*. Briefly speaking, *individual verification* permits voters to check that their individual ballots are correctly cast and counted.

From a system viewpoint, *universal verification* allows poll workers to inspect that the election results correspond to the cast ballots. The aim is to ensure that the whole voting process is performed correctly, what leads to *trustful* election results. In traditional voting systems, both verifications are achieved by a set of *procedures* (i.e., manual operations addressed by election officials, or also by independent entities and observers from candidates). Contrariwise, a mix of *procedures and technologies* usually addresses them in e-voting systems.

A later enhanced property is the *end-to-end* (E2E) *verifiability*. Seen from a voter's point of view, in an E2E verifiable voting system, a voter can check during the voting process that both her ballot is correctly cast and counted in the final tally. The goal is then to

increase the voters' *reliability* in the election results. Note that this property was hardly supportable in traditional voting systems, since the voter Alice concluded her interaction with the voting system when casting the ballot into the ballot box. However, new designs of voting systems and modern technologies facilitate an E2E voter-verifiable voting process.

In this survey, *we present a fair comparison on the verifiability of electronic voting systems based on poll sites*. We also name them *voting verification systems* (VVSs). The motivation is that poll-site-based voting systems are the most common ones nowadays. Besides, we specialize our study on e-voting systems since they are the most recent trend in democratic voting systems [Ev09]. The systems included in this analysis are remarkable commercial and academic solutions of the last decade. Thus the contribution of this work is twofold: (i) definition of a *common evaluation framework* to fairly compare all systems and (ii) *study and comparison* of remarkable e-voting systems.

Document structure The next section introduces the necessary background for the present work. Sec. 3 presents the evaluation framework and Sec. 4 the analysis of all voting verification systems (VVS). In Sec. 5, we perform the analysis of all the systems and pinpoint the technological trends. Finally, Sec. 6 presents the concluding remarks of this work and some future work.

2 Background

We consider in this study the standard voting process composed of the following phases: (i) *voter registration* and identification, (ii) *vote casting* using ballots and (iii) *vote tally*, where all ballots are securely *tabulated* and unbiased results are made *public*. The voting process also includes all *procedures* and *technologies* to trustfully address the consultations or elections. In addition, we present the system classification of the voting models and voting verification systems, according to the voting location and the U.S. HAVA classification, which will be used later in this work to organize the analyzed voting systems.

2.1 Voting models

We present two classifications of the voting models, according to the place where voters have to attend to vote (see Sec. 2.1.1), as well as according to the U.S. HAVA classification (see Sec. 2.1.2).

2.1.1 Location-based classification

According to the place voters have to go to vote, voting systems are broadly classified into **poll-site-based** and **remote** voting systems. The former type is the most used nowadays, and it is characterized by having voters go to specific buildings, namely poll sites, to cast their votes. Conversely, voters may remotely cast their vote in *remote voting systems*. The most important examples are **vote-by-mail** and **internet voting.**

Recently, a new kind of systems has been proposed: **presential remote**. Such systems allow the casting of votes in a controlled environment (i.e., poll sites) although the tally is electronically conducted at a centralized site, dedicated to securely count all votes. Therefore, this kind of systems benefits from both existing modes, poll-site-based and remote, since they are very helpful when voters are abroad (e.g., the military), whilst at the same time reducing the tally time.

As mentioned earlier, our *focus* is put *on verification systems of poll-site-based systems*, which also allow us to take presential remote voting systems into consideration.

2.1.2 HAVA classification

This classification has been promulgated by the Election Assistance Commission (EAC), an independent agency of the United States government created by the Help America Vote Act of 2002 (HAVA). Appendix C of the 2005 VVSG [El05] separates the VVSs into four types: (i) **process separation-based** VVSs have a modular architecture split into two independent, totally isolated systems dealing with the *generation* and *casting processes, respectively*; (ii) **evidence-based** VVSs are based on capturing *all actions* performed during the voting phase of voters; (iii) **direct** VVSs generate a *parallel* registry of votes, which permits a direct verification of the vote to be cast; lastly, (iv) **end-to-end cryptography-based** VVSs employ cryptographic methods to craft receipts which allow voters to verify that their votes were not modified, without revealing the voting preferences of the voters. We will classify the evaluated electronic VVSs using this classification system.

3 Common Evaluation Framework

In this section, we introduce the classification and properties that we will extract from the set of systems under consideration. All of them constitute the single, structured *evaluation framework* that we will use to ease their fair comparison and analysis.

3.1 Classification of VVSs

We employ the following classification to *percolate* the systems through, respectively, in order to obtain their natural organization. The publication year of the academic publication or system is the last organizational property used.

1. From **electronic-** and **paper-based systems**, we only consider electronic VVSs, which require voting in an *electronic* (instead of a *paper)* format.

2. We use the aforementioned **HAVA classification** to separate them into *process separation-*, *evidence-*, *end-to-end (E2E) cryptography-based* and *direct* VVSs.

3. We further organize them into **integral** or **independent systems**. *Integral* ones perform the whole voting process, while *independent* VVSs are designed solely to verify independently that another voting system's operations can be trusted.

3.2 Evaluated properties from VVSs

We present in this section the characteristics considered against which all systems are to be evaluated. We have classified them into these voting process concerns: *user interaction*, *security*, *integrability* (with an existing voting system), as well as *technical issues*. Note that any property definition is such that a *positive answer* corresponds to a *positive feature*.

User interaction The *user interaction* greatly determines the voters' impression and *reliability* of the voting system:

1. **Accessibility** Whether the system *does not* prevent a disabled user to vote.

2. **Use impact** Whether the system *does not* create a more complex (even longer) process to cast a vote.

3. **Reliability** Trust in the whole voting process from a *voter's viewpoint*.

Security The security issues are broadly categorized into these two big sets, namely *voter* and *voting process*:

Voter-related:

4. **Ballot secrecy** The system *prevents* a third entity from seeing the contents of the ballot.

5. **Voter anonymity** The system *prevents* the ballot from being linked to the voter.

6. **Coercion resistant** A coercer *cannot* verify nor demonstrate how the voter voted.

7. **Individual verification.** A voter *can* verify that her vote was accounted for *properly*.

Voting-related:

- **Universal verification:**

8. **Ballot box integrity** Only registered voters' votes *appear* at the end of the voting process (before the tally process) and are unmodified.

9. **Tally accuracy** The tally process *counts* all of the cast votes and not before the end of the voting process (i.e., no partial results are allowed).

10. **Auditability** The e-voting system (with no paper trails) *allows* a third party to analyze what happened before, during, and after the vote was cast, without compromising other security properties, in order to certify the final tally and election results.

Integration Regardless of whether the VVSs are *integral* or *independent*, we will consider the feasibility and effectiveness of adapting/integrating the evaluated system with other voting systems. In particular, briefly speaking, we consider the synchronization of operations, especially when votes are being cast, between a given voting system and the evaluated system *acting as an independent VVS* (as issued in [Sh06]).

11. **Integration** *Ease* of implementing/adapting the evaluated system as an independent verifier system for other voting infrastructures.

12. **Data management** Whether the vote cast subsystem of the voting systems and the evaluated system *guarantee* atomicity, as well as whether this integration is resistant to failures (e.g., user errors, cable disconnections).

Technical issues We also analyze the VVS performance from a *technical viewpoint*:

13. **Simplicity** Whether the verification solution *is* straightforward and simple.

14. **Availability** A suitable voter *must be able to* cast her vote, within the established time period, and be prevented from voting multiple times (if not otherwise allowed).

15. **Scalability** The verifier system computationally *scales*.

16. **Flexibility** This measures the level of freeness *allowed* by the verifier system (e.g., number of candidates, write-in mode).

Properties representation For brevity, when summarizing these sixteen properties for all the evaluated systems, we will use the following notation:

User interaction	↑/↓/~: Good/Weak/Acceptable.
Security	**Y**/**N**/~: **Y**es/**N**o/Partially.
Integration	**NT**: **N**o additional **T**echnical requirements (on voting consoles, etc). **T**: Additional **T**echnical requirements. **NSW**: **N**o additional **S**oft**W**are requirements (on voting consoles, etc). **SW**: Additional **S**oft**W**are requirements.
Data management	**NA**: There is **N**o operation **A**tomicity. **A**: There is operation **A**tomicity. **DL:** There is **D**ata **L**oss. **NDL:** There is **N**o **D**ata **L**oss.
Technical Issues	↑/↓: High/Low
At any property	"N/A": When the property is *not addressed*.

Table 1: Value representation of the considered evaluation properties

4 Presentation and classification of VVSs

We present here all the evaluated *electronic VVSs*. The idea behind them is that they depend primarily on e-voting procedures, even though some of them may have paper *receipts* to provide E2E verifiability. From the HAVA classification, we present solutions on three out of the four types: *process separation-*, *evidence-,* and *end-to-end cryptography-based* (E2E).

4.1 Process separation-based VVSs

As we have presented before, a process-separated VVS is divided into two independent and isolated subsystems: *ballot generation* and *casting*. In this class of systems, the security constraints are mainly applied to the casting process. We present below the most representative one: Modular Voting Architecture, namely "Frog" [BJR01].

4.1.1 Modular voting architecture ("Frog")

S. Bruck, D. Jefferson, and R. Rivest presented this system in 2001 [BJR01]. It is the example *par excellence* of separation process and, therefore, it implements an integral e-voting solution that emphasizes and standardizes a separation between vote *generation* and vote *casting* components.

On the day of the election, the voter identifies himself to a poll worker, who takes a blank *ballot* (ballots are named *frogs*), initializes it and, then, returns the ballot to the voter. Afterwards, the voter inserts his ballot into the *vote generation equipment*; she selects her options through a direct-recording electronic (DRE) voting machine, and her

choices are introduced onto her ballot. The second phase starts here. The voter introduces her ballot into the *vote-casting equipment* and *checks* the content of her ballot. When the voter agrees with the content, her ballot is digitally *signed* (using a single key for all votes), then *frozen* (the frog is blocked against writing), and finally *deposited* into the *frog bin*. At this moment, an electronic copy of her vote is randomly stored in a data unit memory and replicated in other memories for reliability. Once the elections are over, election officials publish the results for each precinct in a Web as two separated, unlinked lists: one with the voters' names and the second one with all cast ballots with a system-wide digital signature. Therefore, anyone can verify the digital signature and compute the election results.

4.2 Evidence-based VVSs

These systems capture the actions performed by voters when casting their votes, independently of the voting system and invisible by the voter. In addition, to ensure information integrity, all recorded events are stored outside of the vote terminal. Under this type of VVSs, we consider VVAATT and VVVAT.

4.2.1 Voter verified audio audit transcript trail (VVAATT)

VVAATT is an *audio verification* system, introduced by T.Selker and S.Cohen in 2004 [Se04, SC05]. This system records the *audio* of all events during the voting process into a physical medium (in a cassette tape or in a CD-W media), at the same time this is complemented by the *visual* verification from the DRE. In the same line, there exists Voter Verified Video Audit Trail (VVVAT), which instead, captures the sequence of screenshots on the DRE terminal (see [Cr07] for an example).

4.3 End-to-end verifiable VVSs

We present in this section the E2E cryptographic-based VVSs, which among other capital properties have an end-to-end (E2E) verifiability. To do so, some of them generate *paper receipts* to allow voters to check that their votes were counted in the tally process. The following solutions are the selected systems under analysis: VoteHere [Ne01], VoteBox [SDW08], Three-Ballot-Based Secure Electronic Voting System [SCM08], and the last ErgoGroup/Scytl proposal [No09b].

4.3.1 VoteHere

VoteHere is an integral solution introduced by C. Andrew Neff and VoteHere, Inc. in 2001 [Ne01, Va01]. This system is based on the use of DRE terminals. It is built considering receipt- and cryptography-based verifications in order to cover both *individual* and *universal* verifications.

For each voter, the voting system builds a *code* for each electable candidate before the election starts. Once the voter has chosen her preferences on the DRE, the DRE shows

the codes related to each candidate. If they correspond with those pre-built codes, the voter confirms her vote and a *receipt* is printed with her *verification codes*. Once the election ends, the *encrypted votes* are made publicly available (guaranteeing ballot secrecy), and then the voter can *check* if her vote was counted (or complain to election officials otherwise).

4.3.2 VoteBox

VoteBox is an integral solution and was developed by D. Sandler, K. Derr, and D. Wallach in 2008 [SDW08]. The VoteBox system uses a technique adapted from Benaloh's work on voter-initiated auditing [Be07] to gain *end-to-end verifiability*. In other words, the voting system actually is an audit system that records everything that happened. Its main properties are as follows:

- **Pre-rendered user interface** The user interface is built from *pre-rendered* graphics, a closed sequence of pages (screens) containing text, and graphics that reduce runtime code size. The only interactive elements are buttons, rectangular regions of the screen (VoteBox supports touch screens), and other assistive technologies (computer mice, keyboards or audio feedback to state transitions).

- **Tamper-evidence and replication** A *permanent*, *tamper-evident* audit system records the events along the voting process and provides resistance to data loss in case of failure or tampering. VoteBox consists of two parts: the supervisor console and VoteBox booths (i.e., voting terminals). A broadcast network connects both parts, so that events from both parts (including ballot casts or supervisor commands) are replicated on all voting terminals and entangled with a hash chaining to provide *immutable* logs.

- **End-to-end verifiability** To encrypt ballots, VoteBox uses the ElGamal cryptosystem and its *additive homomorphic* property. Any cast ballot is encoded in a binary format and encrypted by a public key for the election. Therefore, the tally is addressed by (i) the multiplication of all ballots and (ii) the multiplication result decryption in order to obtain the election results.

4.3.3 A three-ballot-based secure electronic voting system

This system [SCM08] is based on the original, paper-based Three-Ballot system [Ri06], but is completely redesigned to provide a full electronic solution. The idea behind the Three-Ballot approach is that a *ballot* consists of three single *parts*, with a list of candidates in the same order on the three parts. In order to vote for a candidate, the voters mark *any two parts* for the corresponding candidate (marking only one part means no vote is cast). When casting the vote, the three parts are separated from each other and mixed with the rest of parts from other voters. The tally operation is done by a simple calculation on the number of marks for each candidate on all the parts. One out of the three parts is randomly chosen by the voter to *copy* and to take home as a *receipt*. The same approach is maintained in this electronic version of Three-Ballot [SCM08].

4.3.4 E-valg 2011

The Norwegian Ministry of Local Government and Regional Development initiated in 2008 a selection process of e-voting technological providers, which finished on December 2009. ErgoGroup[1] and Scytl[2] [No09b] will provide the e-voting solution for the Norwegian municipal elections in 2011 [No09c].

The ErgoGroup/Scytl's solutions provide all the security requirements by using cryptographic techniques. Until now, the ErgoGroup/Scytl consortium has designed various systems to support two types of voting: *poll-site-based* (compatible with DREs) [Sc04] and *remote voting* [PM07]. Moreover, the latter allows a presential remote voting model, which suits the system requirements specification of the E-valg 2011 project [No09d].

ErgoGroup/Scytl's proposal [No09b] is based on a *hybrid scheme* that combines mixing techniques and ElGamal homomorphic properties [Pe09]. The homomorphic cryptography uses a *multiplicative* property [Pe04, Pe09] so that the system performs partial multiplications of the votes. The election private key, used to open the encrypted votes, is generated using a *threshold scheme* [Sh79]. Lastly to retain all desirable security properties, this system uses digital signatures, zero knowledge proofs, and the generation of return codes (i.e., *receipts*).

5 Study and comparison of VVSs

In this section we introduce the analysis of the considered VVSs (Sec. 5.1) and the study of the synergies on voting systems and cryptographic technologies (Sec. 5.2).

5.1 Analysis and comparison of VVSs

We follow the properties considered in our common evaluation framework to compare and analyze all evaluated VVSs. See Tab. 3 for the complete elaboration.

User interaction Given that all VVSs use DREs to emit votes, all of them provide a certain degree of **accessibility**. However, some of them improve it by using audio guides (VVAATT), or indeed with other assistive technologies (such as mice or keyboards) (VoteBox and E-valg). For the E-valg case, this is proved by the studies [Sh06], [No09a]. As for the **use impact**, systems like Frog, VoteBox and Three-Ballot present a more complex and likely longer voting process. For instance, in Frog there exists a strict separation of the generation and cast processes (even though a voter can bring a filled ballot from home); VoteBox allows voters to perform an "immediate ballot challenge" [Be07]; and Three-Ballot uses a multi-ballot composed of 3 parts. Further, in order to increase the **reliability** of the voting system, they provide three kinds of augmented features: (i) frogs (Frog) and *receipts* (VoteHere, VoteBox, Three-Ballot and E-valg)

[1] http://www.ergogroup.no/default.aspx?path={2A1C0F50-F200-43C8-98C6-36CD82F7A587}
[2] http://www.scytl.es

tangible elements for the voter, (ii) audio guides (VVAATT), and (iii) public web bulletins (all except VVAATT).

Security VVAATT/VVVAT do not ensure vote confidentiality, given that all (audio or video) recordings show the *sequential* voting order. In addition, VVAATT/VVVAT suffer from *weak* recording equipment protection (given that they must be accessed often) and *untrustworthy* information extraction techniques. In conclusion, even though the recording support provides audit means, VVAATT/VVVAT are not reliable. Next, we only will focus on the rest of the systems.

Voter-related security Except for Frog, all of the systems use a public key infrastructure (PKI), most of them ElGamal, to ensure **ballot secrecy**. However, these VVSs use very different techniques to guarantee **voter anonymity**. While Frog uses a simple randomization algorithm, Three-Ballot separates each of the three parts of a ballot and stores them using their hash values. More complex techniques also appear: mixing (VoteHere), additive homomorphism (VoteBox) or a hybrid scheme (multiplicative homomorphism and mixing in E-valg). VoteBox, Three-Ballot and E-valg are **resistant to coercion and vote selling**. The same is not true for VoteHere, since it may have a flaw given that it shows both encrypted ballots and receipts with return codes [Ba04]. Lastly, except for Frog, all systems render *augmented* **individual verification** with *E2E* voter *verifiability* through receipts.

		Security Techniques			
		ZKPs	Digital Signatures	Threshold Scheme	Audit System
VVS	Frog	No	Yes	No	No
	VoteHere	Yes	Yes	Yes	No
	VoteBox	Yes	Yes	Yes	Yes
	Three-Ballot	No	Yes	No	No
	E-valg	Yes	Yes	Yes	Yes

Table 2: Security techniques used by voting verification systems

Voting-related security Except for Frog, all of the systems ensure **ballot box integrity** through different technologies (like ZKPs, digital signatures or threshold schemes). The use of a threshold scheme prevents security attacks against the electoral system. See Tab. 2 for more details. Thus, VoteHere, VoteBox, Three-Ballot and E-valg guarantee **tally accuracy**. Homomorphic algorithms make a more efficient tally than mixing techniques [Pe04, Pe09]. As for **auditability**, Three-Ballot creates logs for any voter-related operation, even though it creates none about the tally process. The evaluated strongest audit systems appear in VoteBox and E-valg, which use *immutable* logs. VoteBox, however, builds a distributed total audit system, while E-valg only centrally audits the critical system elements.

Integration In order to be **integrated**, the evaluated VVSs have some software or technological dependences (see Tab. 3 for more details). However, only VoteBox and E-valg [Sh06] ensure vote atomicity, loss resistant, and tamper evident solutions.

Technical issues VoteBox and Frog are more **complex** than the rest of the systems, given that the former has a distributed infrastructure, and the latter is strictly tied to the separation of processes. However, VoteBox is the only system that structurally provides distributed *replication* of sensible information, which leads to a high degree of system **availability**. Another of VoteBox's good properties is its **scalability**, given that it uses homomorphic cryptography, and thus makes the tally process easier. This property is also shared by E-valg. However, both of them should carefully address presential remote voting, guaranteeing the necessary infrastructure in order not to overload the voting system. Finally, only Frog, VoteHere and E-valg render **flexible** on vote type and format. Notice that VoteBox, by using additive homomorphic cryptography, only supports simple types of votes. Lastly, Three-Ballot is only suitable for multi-ballot formats composed of 3 single parts, even though that the ballot content is flexible.

5.2 Study of trends in VVSs

From the above analysis we can extract *three clear trends* in regard to the following issues: (i) voting location, (ii) voting technology, and (iii) degree of verifiability.

Voting location study We have evaluated *poll-site-based* VVSs. All of them use DREs as voting terminals. Clearly, DREs are very helpful in order to manage votes electronically. It is worth noting the demonstrated trend away from *poll-site-based* toward presential remote voting systems. For instance, VVAATT/VVVAT, Frog, VoteHere and Three-Ballot are of the first type, and VoteBox and E-valg are presential remote voting systems. This trend is a consequence of not only the technology, but also the natural evolution in the democratic rules. However while VoteBox was *adapted* to support presential remote voting schemes, E-valg was *structurally* designed to do so.

Voting technology study We consider here the voting technology used from the ballot cast to the tally and, therefore, VVAATT/VVVAT-based systems are not considered. The idea behind this technology is to address security issues such as voter anonymity, ballot box integrity, and tally accuracy among others. These systems present a clear evolution in this issue. We detail them from simpler to more complex and reliable solutions.

While Frog uses only a simple *randomization* algorithm to anonymize votes, VoteHere uses a more reliable mixing technique to address *voter anonymity*. VoteBox and Three-Ballot use (computationally hard) *additive homomorphic* cryptography to guarantee *voter anonymity* and to perform the *tally*. The most complex, but flexible and reliable technology is used by E-valg, the *hybrid scheme*, which is composed of multiplicative homomorphic cryptography (computationally less hard than additive ones [Pe04, Pe09]) and mixing mechanisms. Clearly, the technology used presents a *trade-off* between ensuring (i) more secure, trustful, and reliable voting technologies, and at the same time guaranteeing (ii) fast and resource-efficient ones. This trend from simple randomization techniques to hybrid schemes is a direct consequence of the continuous permeability of voting systems with regard to the latest cryptographic advances.

Verifiability study We can organize the analyzed systems as follows: (i) VVAATT/VVVAT-based and Frog systems provide deficient or basic verifiability in voting processes, respectively. They mainly guarantee at some degree the individual verifiability, yet the same is not true for universal or E2E verifiability. (ii) VoteHere and Three-Ballot VVSs offer an acceptable degree of verifiability (individual, universal, and E2E). Finally, (iii) E-valg and VoteBox ensure a good level of verifiability, while at the same time they define a tough audit system. To sum up from all of these remarkable VVSs, VoteBox and E-valg are the best alternatives for voting systems. However, E-valg is a better voting system candidate, which should be followed closely. This is because it provides commercial applications, a high degree of verifiability, and a smooth transition from traditional voting systems to electronic ones, not to mention its accessibility and ease-of-use.

VVS	USER INTER.			SECURITY							INTEGR.		TECHNICAL ISSUES			
				VOTER-RELATED				VOTING-RELATED								
								UNIVERSAL VERIFICATION								
	Accessibility	Use Impact	Reliability	Ballot Secrecy	Voter Anonymity	Coercion Resistant	Individual Verification	Ballot Box Integrity	Tally Accuracy	Audtability	Integration	Data Management	Simplicity	Availability	Scalability	Flexibility
Frog	↓	~	↑	N	Y	N	~	~	N	N	SW/T	N/A	↓	N/A	↓	↑
VVAATT	~	↑	↑	N	N	N	N	N	N	~	T	DL/NA	↑	N/A	↓	↓
Vote Here	↓	↑	↑	Y	Y	N	Y	Y	Y	N	SW	N/A	↑	N/A	~	↑
Vote Box	↑	↓	↑	Y	Y	Y	Y	Y	Y	Y	SW/T	NDL/A	↓	↑	↑	↓
Three-Ballot	N/A	↓	↑	Y	Y	Y	Y	Y	Y	Y	N/A	N/A	↑	N/A	~	↓
E-valg	↑	↑	↑	Y	Y	Y	Y	Y	Y	Y	N/A	NDL/A	↑	N/A	↑	↑

Table 3: Detailed properties of the Voting Verification Systems.

6 Conclusions

In this paper, we have presented an evaluation framework, common for all systems, in order to conduct a fair study of the different electronic voting verification systems (VVSs). The strong point of the present study is threefold: (i) we define the common evaluation framework, (ii) we present academic and commercial VVSs, and (iii) we conduct a fair study and comparison among them, having the verifiability analysis as a connecting thread.

Even though the origin of e-voting systems was to accelerate the tally process, the trend is clear and firm towards not only electronic tally, but also electronic vote casting

[Ba06]. Since the introduction of the DREs, more and more initiatives are addressing electronic casting in elections. This trend is also visible in our study.

As we have seen, good designs of e-voting systems may be significantly helpful for disabled and also for illiterate citizens. At the same time, the use of electronic voting technologies may reduce the economic and logistic costs of elections and consultations, while facilitating geographically distributed citizens to vote. Even though there are no conclusive studies, the tally accuracy on e-voting systems is higher than in paper-based voting systems [Ba06]. However, e-voting systems should not be massively introduced – education and increasing the sensibility toward democracy is necessary beforehand– in a society where there exists a high ratio of abstention.

As demonstrated by the technologies used in the latest e-voting systems, we foresee that the future trend in the use of electronic voting will be *remote e-voting*. In this line, there were some first *remote presential* and *internet voting* experiences. The global acceptation of these remote e-voting schemes will empower citizens with new democratic participation tools, which will likely lead to direct and binding citizen consultations and elections.

Bibliography

[Ba04] Barnes, Richard. 2004. VoteHere VHTi. A verifiable e-voting protocol. Cryptography applications bistro. http://www.cs.virginia.edu/crab/VoteHere.pdf/. (accessed Feb. 2010).

[Ba06] Barrat Esteve, Jordi. 2006. A preliminary question. Is e-voting actually useful for our democratic institutions? What do we need it for? In *Proc. of 2nd international conference on electronic voting (E-VOTE '06)*, 51–60. GI, Bregenz, Austria.

[Be10] Bellis, Mary. 3rd November 2009. The history of voting machines. http://inventors.about.com/library/weekly/aa111300b.htm/. (accessed Feb. 2010).

[Be07] Benaloh, Josh. 2007. Ballot casting assurance via voter-initiated poll station auditing. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07)*, 14–14, Berkeley, CA, USA: USENIX Association.

[BJR01] Bruck, Shuki, David Jefferson, and Ronald Rivest. 2001. *A modular voting architecture ("Frogs")*. In Proceedings of the Workshop on Trustworthy Elections (WOTE '01), California, USA. URL: http://vote.caltech.edu/backup/wote01/pdfs/amva.pdf

[Cr07] Cross, E.V., G. Rogers, J. McClendon, W. Mitchell, K. Rouse,P. Gupta, P. Williams, I. Mkpong-Ruffin, Y. McMillian, E. Neely, J. Lane, H. Blunt, and J.E. Gilbert. 2007. Prime III: One machine, one vote for everyone. In *(On-line) proceedings of 2007 voting competition conference*. http://vocomp.org/papers/primeIII.pdf/. (accessed Feb. 2010)

[El05] Election Assistance Commission (USA). 2005. Voluntary voting system guidelines. http://www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf/attachment_download/file/.

[Ev09] E-voting.cc (competence center for electronic voting and participation). 2009. Map of electronic democracy. *Modern Democracy* 2(1):8–9.

[Ne01] Neff, C. Andrew. 2001. A verifiable secret shuffle and its application to e-voting. In *CCS '01. Proceedings of the 8th ACM conference on computer and communications security*, 116–125. New York, NY, USA: ACM.

[No09a] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Accessibility and usability evaluation of e-vote prototypes. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf/. (accessed Feb. 2010).

[No09b] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Contractor solution specification. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/Tilbud_ergogroup/SSA-U_Appendix_2A_Contractor_Solution_Specification.pdf/. (accessed Feb. 2010).

[No09c] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Project directive for e-valg 2011. http://www.regjeringen.no/upload/KRD/Vedlegg/KOMM/Evalg/Project_directive_evalg2011_v101_english.pdf/. (accessed Feb. 2010).

[No09d] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. System requirements specification. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System_Requirements_Specification1.pdf/. (accessed Feb. 2010).

[Pe04] Peng, Kun, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee. 2004. Multiplicative homomorphic e-voting. In *Proceedings of 5th international conference on cryptology in India (INDOCRYPT '04)*, 61–72. Kolkata, India. Springer.

[Pe09] Peng, Kun. 2009. A hybrid e-voting scheme. In *Proceedings of the 5th international conference on information security practice and experience (ISPEC '09)*, 195–206, Berlin, Heidelberg: Springer-Verlag.

[PM07] Puiggali, Jordi, and Vitor Morales-Rocha. 2007. Independent voter verifiability for remote electronic voting. In *Proceedings of international conference on security and cryptorgraphy (SECRYPT '07)*, 333–336. Barcelona, Spain. Springer.

[Ri06] Rivest, Ronald L. 2006. The three-ballot voting system. Unpublished draft.

[Sc04] Scytl Online World Security S. A. 2004. Auditability and voter verifiability for electronic voting terminals. http://www.scytl.com/_a_home/PNYX.VM_White_Paper.pdf. (accessed Feb. 2010).

[SC05] Selker, Ted, and Sharon Cohen. 2005. An active approach to voting verification. http://vote.caltech.edu/drupal/files/working_paper/vtp_wp28.pdf/. (accessed Feb. 2010).

[SCM08] Santin, Altair O., Regivaldo G. Costa, and Carlos A. Maziero. 2008. A three-ballot-based secure electronic voting system. *IEEE Security and Privacy* 6(3):14–21.

[SDW08] Sandler, Daniel, Kyle Derr, and Dan S. Wallach. 2008. Votebox. A tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th conference on security symposium (SS'08)*, 349–364. Berkeley, CA, USA: USENIX Association.

[Se04] Selker, Ted. 2004. The voter verified audio audit transcript trail. http://www.dos.state.pa.us/election_reform/lib/election_reform/VVAATT_CalTech.pdf/. (accessed Feb. 2010).

[Sh79] Shamir, Adi. 1979. How to share a secret. *Commun. ACM* 22(11):612–613.

[Sh06] Sherman, Alan T., Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, Donald F. Norris, John Pinkston, Andrew Sears, and Dongsong Zhang. 2006. An examination of vote verification technologies: findings and experiences from the Maryland study. In *Proceedings of the USENIX/accurate electronic voting technology workshop 2006 on electronic voting technology workshop (EVT'06)*, 10–10. Berkeley, CA, USA: USENIX Association.

[Va01] Varner, Philip E. 2001. Vote early, vote often, and vote here. A security analysis of VoteHere. PhD diss., University of Virginia.

Sigma Ballots

Stefan Popoveniuc[1] and Andrew Regenscheid[2]

[1]KT Consulting
Gaithersburg, MD, USA
stefan@popoveniuc.com

[2]Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD, USA.
andrew.regenscheid@nist.gov

Abstract: We present Sigma ballots, a new type of ballot designed to be used in secure elections. Sigma ballots use the random order of candidates introduced by Prêt à Voter, combined with the confirmation codes of Scantegrity II. These ballots can be produced by a DRE machine with a slightly modified VVPAT, or can be similar to optical scan ballots. Sigma ballots work in conjunction with existing publicly verifiable tallying schemes to allow for end-to-end verifiability. The advantages of Sigma ballots include an easy check for correct printing, the possibility of keeping a fixed order of candidates when selections are made, automated creation of receipts, no extra marks added to the ballot after it is cast, the ability to be hand counted, and voters only needing to know a valid confirmation code to file a complaint.

1 Introduction

A new class of voting systems was developed in the last couple of years which allows for a unique level of public scrutiny of the declared totals. These systems, known as *end-to-end verifiable voting systems*, allow voters to check that their ballots were cast and recorded as they intended, and allow anyone to check that all the recorded ballots have been correctly tallied. They offer security properties radically different from any voting system used in elections today.

While, in theory, many end-to-end verifiable voting systems have great properties, in practice, they suffer from known weaknesses. Some of them may be difficult to use by voters [PH06], others may be difficult to implement in practice [CD04], some may be too slow for very large elections [CRS05], while others may be vulnerable to attack [CD08].

Recently, binding elections have been run using end-to-end verifiable systems [EA07, AB09]. Scantegrity II [CD08] has been used in a public election, to elect the mayor and city council of Takoma Park, MD. While Scantegrity II has many desirable security properties, it suffers from a series of problems, many of them being acknowledged after the Takoma Park election.
In this paper, we present Sigma ballots, a new type of ballot which can be used in conjunction with existing publicly verifiable tallying schemes to create end-to-end verifiable voting systems that are not vulnerable to many attacks faced by existing systems.

1.1 Motivation and Related Work

A number of end-to-end verifiable voting systems have been proposed [EA07, AB09, CD08, AR06, CRS05]. Many of these systems have known vulnerabilities.

A well-known attack on Scantegrity II is to misprint the ballots. For example, if we assume that a certain voter is going to vote for Alice, but the inside attacker is a supporter of Bob, then the attacker may print next to Alice the confirmation code that corresponds to Bob. The voter fills in the oval next to Alice's name and gets a confirmation code that she thinks is for Alice, when in fact it is for Bob. The tallying mechanism is going to correctly transform this confirmation code into a vote for Bob. This attack is possible because voters are not able to directly distinguish improperly printed Scantegrity II ballots from correctly printed ones.

The typical way of mitigating this attack is to allow the voter to choose two ballots, one to vote, and one to spoil and audit the printing on it. This approach is theoretically sound, but in practice there are multiple disadvantages. First, the approach adds time and complexity to the voting process. Second, voters need to take the fully marked ballots home, and check them against the data on a bulletin board. This potentially violates current election practices, as ballot accounting procedures in many jurisdictions prevent voters from leaving the polling place with a ballot, even spoiled ballots. Third, the approach is highly dependent on procedures followed both by the voter and election officials [KJ07].

Another option is to have a designated auditor that comes and chooses a random set of ballots to be audited for correct printing. This solution requires a trusted auditor, as well as a secure chain of custody for the audited ballots.

The same print audit problem exists in other voting systems, e.g., Prêt à Voter [CRS05], Scratch&Vote [AR06], or, more generally, voting systems in which the ballot does not consist of two or more symmetrical parts, such as PunchScan [PH06].

Another issue with Scantegrity II is that voters are asked to create their receipts by hand. They have to write down the serial number of the ballot along with the confirmation codes for each ballot question. This task can be time consuming and error-prone.

A third security problem identified with Scantegrity II is the possibility of the voting system transforming a no-vote into a valid vote, or a valid vote into an over-vote, by adding extra marks to the ballot after it was cast. Since the voter cannot prove that she does not know the codes for the marks she did not make, the voter cannot prove that she was not the one that made the marks which were in fact added by the system afterwards. This security issue is unique to end-to-end verifiable voting systems where the voting receipt is a proof of knowledge, rather than a partial copy of a cast ballot.

1.2 Contribution

This paper presents Sigma ballots, a new type of ballot to be used to create secure voting systems. Sigma ballots use the random order of candidates introduced by Prêt à Voter, combined with the confirmation codes of Scantegrity II. These ballots can be produced by a DRE machine with a slightly modified Voter Verifiable Paper Audit Trail (VVPAT) printer, or can be similar to optical scan ballots. For illustration purposes this paper provides an example (see section 5) for how to implement verifiable ballot tallying using techniques from Scantegrity II [CD08].

Similar to PunchScan, but without suffering from its indirection problems, the proposed Sigma ballots are two parts symmetrical ballots, with any of the parts containing the same amount of information. The voter may use any of the parts to check for correct printing, without being able to prove how she voted.

Sigma ballots can be used to automatically create a receipt, without the voter needing to write down anything by hand.

Sigma ballots also solve the problem of improperly invalidating cast ballots by giving the voter a digitally signed receipt, covering all and only the selection on the voter's ballot. The voter can now prove that extra marks have been added to her ballot after it was cast by presenting her signed receipt.

2 Description of Sigma ballots

We start by describing what a Sigma ballot looks like. In section 3, we detail how the Sigma ballot can be created using either a DRE with a VVPAT printer, or an optical scan system.

The design of the Sigma ballot uses ideas from the Prêt à Voter ballot and the Scantegrity II confirmation codes. Sigma ballots are filled-in ballots, clear text, with marks next to the candidates the voter selected. Voters can inspect a Sigma ballot to verify that their choices are correctly represented, by checking the names next to the marks. Also, Sigma ballots can be counted by hand.

Figure 1 shows a Sigma ballot. On the left side of the ballot is a list of candidates, in a permuted order on each ballot[1]. The order of the candidates on each ballot is publicly committed to before the election and may be different for different ballots. On the right, there is a mark for each candidate the voter selected.

The voter can check that the marks appear only next to the candidates she voted for. If not, the voter can start creating another Sigma ballot (no harm was done). This check is similar to asking the voter to verify that the Voter Verified Paper Audit Trail (VVPAT) contains her choice in a DRE+VVPAT system.

Each mark that appears next to the candidates has a confirmation code assigned to it. All the confirmation codes are printed at the bottom of the ballot. A public commitment ties the confirmation code to the marks next to the candidates, i.e., to the position where marks appear at.

Instructions are printed at the bottom of the ballot about how the voter can check that her vote was correctly recorded. There are also two bar codes containing digital signatures. One signature covers the confirmation codes and the order of the candidates (the left side); the other covers the confirmation codes and the position where marks appear at (the right side).

Like in Scantegrity II, the voter only sees the confirmation codes for the candidates she selected, creating a knowledge-based receipt. If the voter notices that her confirmation codes are not correctly posted on the public bulletin board, knowledge of a valid confirmation codes is sufficient to file a complaint.

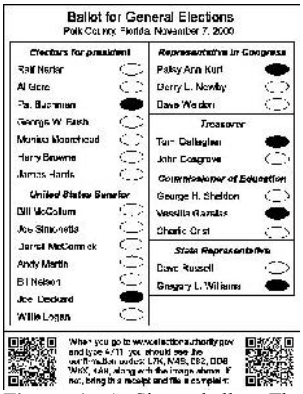


Figure 1: A Sigma ballot. The order in which the candidates are printed may be different on different ballots. The confirmation codes are not associated with candidates or marks.

Figure 2: Receipt produced by photocopier 1. The order of the candidates is visible, but no marks are visible, so an observer cannot tell how the voter voted.

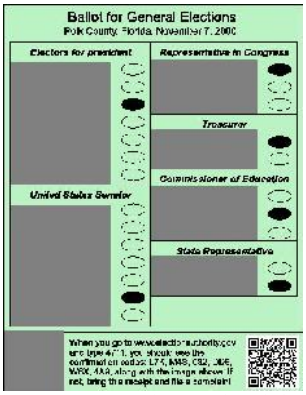


Figure 3: Receipt produced by photocopier 2. The marks are visible, but the order of the candidates is hidden, so an observer cannot say which candidates the marks correspond to.

[1] The name "Sigma ballot" comes from having a permutation represented by the Greek letter σ.

There are two photocopiers in the polling place, which are used to produce a receipt from a Sigma ballot. On her way out, the voter may choose one of the two photocopiers and place her ballot in it. The scanning portion of the photocopiers is partially blackened out by an opaque template (i.e., black tape), such that, for the first photocopier, the template hides (i.e., does not allow to be copied) the portion with the marks (Figure 2). For the second photocopier, the template hides the portion with the order of the candidates (Figure 3). The copy produced by the photocopier becomes the voter's receipt, while the Sigma ballot is deposited into a ballot box.

If the voter chooses the first photocopier, she obtains the order in which the candidates appeared on the voted ballot along with the confirmation codes (see Figure 2). Since no marks for any of the candidates are visible, and since the confirmation codes may be different for different ballots, inspecting this receipt does not reveal the choices the voter made. If the voter chooses the second photocopier, the voter obtains the position of the marks along with the confirmation codes (see Figure 3). Since the order of the candidates may be different on different ballots, the positions where the marks appear do not reveal the chosen candidates. Therefore, no matter which photocopier the voter uses, she gets a receipt that does not reveal how she voted.

The bar code at the bottom of the ballot contains a digital signature of the receipt to avoid voters being able to manufacture fake receipts, and to avoid having the system adding more marks after the ballot is cast. The verification of the correctness of the digital signature is part of future work.

To simplify things, two digital signatures are on the initial Sigma ballot. Depending on which photocopier is used, one of them is covered, such that the receipt only contains the appropriate digital signature.

All the receipts are posted on a public bulletin board and the voter may check it and compare her receipt to the posted one. If the receipt does not appear on the bulletin board, or if it is not correctly posted (e.g., different confirmation codes, different order of the candidates, or different position of the filled-in marks), the voter can show her physical receipt, which is irrefutable proof that the bulletin board contains invalid information. The posted receipts can be used by a publicly verifiable tallying scheme (see section 5) to produce vote totals which are proven to come from the posted receipts, and thus from the choices the voters made.

2.1 Pre-election setup

Before the election, a set of commitments is published for each ballot. For each confirmation code, a commitment that ties the confirmation code to a coded vote is made. The coded vote is the input to a verifiable tally mechanism (can be a mixnet [PH06] or homomorphic tallier [AR06]).

For each ballot, a commitment to the order of the candidates is published before the election. If the voter uses the first photocopier getting her receipt with the order of the

candidates, this commitment is opened, and anybody (not just the voter), can check that the receipt posted on the public bulletin board is consistent with the commitment that ties each candidate with the position it appears at.

Commitments that tie marks at certain marked positions to confirmation codes are also published for each possible marked position. For each confirmation code on each ballot, the system publishes a commitment that ties the confirmation code to the position that should be marked when this confirmation code is printed on the chit. If the voter uses the second photocopier, the system opens the commitment that binds the confirmation code on the receipt to the position of the mark on the receipt. Anybody can check that, on the posted receipts, the marks appear at the positions indicated by the opened commitments and that the confirmation codes do correspond to these positions.

We assume that the system that produces the Sigma ballot does not know a priori which photocopier is chosen by the voter. If, on a particular ballot, the system modifies either the order of the candidates, or the confirmation codes, then the system has a 50% chance of not getting caught (because there is a 50% chance that the voter chooses the photocopier that makes a copy of the part that was not cheated on). Assuming the voters' choices of photocopiers are independent, the probability of not detecting any misprinted ballots decreases exponentially with the number of misprinted ballots.

2.2 Advantages of Sigma ballots

Sigma ballots have three major advantages. First, it should be relatively easy for the voters to check if the paper ballot contains a vote for the candidate that they voted for: locate a mark and simply read the name of the candidate to the left of the mark. Second, by giving the voters the choice to put their ballot in any of the two photocopiers, the voter performs an automatic print audit of their ballot. In some cases the voters check that the order of the candidates is correct, and in the other cases the voters check that the confirmation codes correspond to the marked positions. Third, the voter does not have to create a receipt by hand, since the confirmation code is already printed on the stub of the ballot, which is photocopied and included in the receipt.

Voters that are not interested in getting a receipt can simply ignore the photocopiers and walk out, but not before depositing the Sigma ballot into the ballot-box. To ensure that the ballots are correctly printed, it is not necessary that all voters get a receipt from one of the photocopiers, but only that a statistically significant, unpredictable fraction do.

Depending on the predictability of the confirmation codes, the lack of a paper receipt may *not* prevent the voter from checking the public bulletin board, just like in Scantegrity II. If correct confirmation codes on any given ballot are difficult to guess by voters, then the voter’s knowledge of the confirmation codes may be sufficient to file a complaint if the confirmation code is not correctly posted on the bulletin board. A voter that provides a confirmation code that is unpredictable, and that was previously committed to, has probably discovered that her correctly cast ballot is not correctly posted on the bulletin board.

3 Producing the Voted Ballot

Sigma ballots are ballots that are already filled-in; they already contain the will of the voter. In this section, we present a few ways in which Sigma ballots can be created. One option is to use a DRE connected to a printer (VVPAT). A second option is to have an optical scan paper ballot that is a combination of Prêt à Voter and Scantegrity II ballots.

3.1 Ballot Marking Devices–DREs with VVPAT

Probably the easiest way to produce Sigma ballots is to use a ballot marking device. This device can look like a DRE, where voters can make their selection using a touch screen and have the liberty to choose the ballot language, font size, contrast, etc. The same device can serve multiple ballot styles.

The order in which the candidates are presented to the voter can be standardized and can be the same for all ballots (such that it is consistent with local electoral law). After the voter made all her selections and inspected the review screen, she presses the "Print Sigma Ballot" button. The DRE has a regular office printer attached to it which prints a Sigma ballot. The voter inspects the print-out to see if marks appear next to the candidates she voted for. If this is not the case, she spoils the Sigma ballot and uses the DRE again to make her selections and to produce another Sigma ballot. Otherwise, the voter walks over to the area where the photocopiers are, following the process described in section 2.

The Sigma ballot can be viewed as a Voter Verifiable Paper Audit Trail (VVPAT). But the VVPAT is not printed under glass and the voter can photocopy part of it. The DRE always prints the Sigma ballot, just like it always prints a VVPAT, regardless if the voter will take the Sigma ballot to the photocopier or not. As soon as the Sigma ballot is out of the printer and is inspectable by the voter, the voter can simply memorize the confirmation codes next to the selected candidates. Later, if the voter does not see the confirmation codes on the public bulletin board, she may still file a complaint, and knowledge of the codes may be sufficient. The voter only knows the confirmation codes for the candidates she selected, thus knowing some other valid confirmation code would mean that either the vote guessed the code (which should be difficult if the codes are unpredictable), or the bulletin board contains an incorrect confirmation code.

By looking at the Sigma ballot, the voter gets a receipt based on "something you know," i.e., the confirmation codes. The voter may also get a "something you have" receipt, a paper receipt, if she uses one of the photocopiers. The extra check that the paper receipt allows the voter to do is to ensure that the association between candidates and confirmation codes on her Sigma ballot is correct. This association has two parts: candidates to positions and positions to confirmation numbers. The voter can check that either the order of the candidates is correct, or that the marks are correctly assigned to the confirmation codes.

Because of the digital signature, neither the voting system nor the voter can add more marks to the receipt after it comes out of the photocopier. Having a physical receipt (as opposed to a "something you know") precluded the voting system from adding more marks to the cast ballots, which may be used as an attack to transform a blank ballot into a voted one, or a voted one into an over-voted one (as is the case in Scantegrity II).

At the end of the voting day, the DREs can provide tallies for fast reporting. Moreover, the Sigma ballots can be used in a hand recount, since each Sigma ballot is a clear text ballot. A third count is provided by an existing publicly verifiable tallying mechanism such as the ones used by Scratch&Vote [AR06], PunchScan [PH06] or the Scantegrity II [CD08] (presented in section 5).

3.1 Optical Scan

A Scantegrity II [CD08] ballot is an optical scan ballot in which, next to each candidate there is an oval printed in invisible ink. The voter fills in the oval next to her desired candidate, and the chemicals in the pen react with the invisible ink printed in the oval, such that the ovals turns mostly black, except for a confirmation code that stays white, and thus becomes visible. The voter can record the confirmation code, in essence creating a receipt for her vote. The paper ballots can be scanned or counted by hand.

A practical problem with a Scantegrity II ballot is ensuring that codes are printed next to the correct candidates. Scantegrity II allows the voter to receive two ballots, one to fully mark and audit the printing on it, and the other one to cast. In practice, since performing the print audit is an extra burden, voters do not perform print audits. In this case, a designated auditor is needed for performing the print audit, which may be problematic.

A Sigma ballot is a Scantegrity II ballot with candidates in randomized order. This solves the print audit problem by allowing the voter to choose one of the two photocopiers to create her receipt and check the correctness of half the printing on her ballot.

Another shortcoming of the Scantegrity II ballots is that voters must create their own receipts, by writing down the confirmation numbers revealed when marking the ovals, or remembering them. Sigma ballots address this too. Assume the voter is allowed to place her Sigma ballot in one of the photocopiers, get her copy, but also get back the Sigma ballot. The voter then deposits the ballot she got back into an optical-scan system, which has a printer attached to it. The voter places the copy she got from the photocopier in the paper feed of this printer, such that the printer will print on this copy. The optical scanner detects the marks from the ballot and prints the confirmation codes on the copy that is in the printer. Therefore the voter does not need to write down the confirmation codes by hand.

The above technique is based on the assumption that the scanner does not know if the voter used the first or the second photocopier (i.e., the photocopier cannot signal the scanner). If the voter used the second photocopier, the copy already contains the confirmation codes, since in a Scantegrity II ballot the codes are revealed when the oval is filled-in by the voter. If the scanner would produce different confirmation codes, then the voter would have irrefutable proof that the scanner printed incorrect confirmation codes. If the voter used the first photocopier, the copy contains the order of the candidate, but without any confirmation codes. In this case the scanner can print incorrect confirmation codes without being detected. But since it is assumed that the scanner does not know what information is already printed on the voter's copy, the chance of printing incorrect confirmation codes and not getting caught decreases exponentially with the number of ballots cheated on.

One can also envision a system in which the scanner is used before the photocopiers: the voter puts the Sigma ballot in a scanner that checks for under-votes and over-votes and also prints the confirmation codes at the bottom of the ballot (a copy of the ballot can also be produced instead of printing at the bottom of the original ballot). Then the voter gets back the ballot and goes to one of the photocopiers, like in the DRE setting. The voter always gets the confirmation numbers, since they were printed by the scanner at the bottom of the ballot. The voter can also check that the scanner wrote the confirmation codes correctly (i.e., it detected the marks correctly), by simply inspecting the output of the optical scanner.

4 Formalization of Sigma Ballots

We present a formal model of Sigma ballots. For simplicity, we model a single race and we assume that there is a candidate "No Vote," which is selected by default if the voter does not select any candidate. Let $\boldsymbol{C}$ be the set of candidates. Let c be the cardinality of the set $\boldsymbol{C}$, and let[2] $\boldsymbol{Z}_c$ be the set of numbers from zero to $c-1$. Let $\boldsymbol{N}$ be the set of all possible confirmation codes, and let $\boldsymbol{E}$ be the set of coded votes that a publicly verifiable tallying scheme takes as input. We assume that the cardinality of $\boldsymbol{N}$ is large.

A Sigma ballot is defined by three functions:

1. $\sigma : \boldsymbol{C} \rightarrow \boldsymbol{Z}_c$ representing the association between the candidates and the position they appear at. σ is a bijective function.
2. $\pi : \boldsymbol{Z}_c \rightarrow \boldsymbol{N}$ representing the association between positions and confirmation codes. π is an injective function. We assume that it is difficult to guess $y \in \boldsymbol{N}$ such that $\exists!\ x \in \boldsymbol{Z}_c$ such that $\pi(x)=y$.
3. $\phi : \pi(\boldsymbol{Z}_c) \rightarrow \boldsymbol{E}$ representing the association between confirmation codes and coded votes. ϕ is an injective function.

A Sigma ballot transforms a clear text vote (a candidate) into a coded vote by composing the three functions $\phi \circ \pi \circ \sigma$.

[2] We abuse the $\boldsymbol{Z}_c$ notation to simply mean the set of numbers from zero to $c-1$ instead of the set of residues modulo c.

The protocol follows the following steps, for each ballot:

1. The election authority computes in secret ϕ, π and σ.
2. The election authority computes and publishes:
    a. A commitment to the entire function σ.
    b. For each $x \in \boldsymbol{Z}_c$, a commitment to $(x, \pi(x))$
    c. For each $x \in \pi(\boldsymbol{Z}_c)$ a commitment to x
    d. For each $x \in \pi(\boldsymbol{Z}_c)$ a commitment to $(x, \phi(x))$
3. The election authority prepares a publicly verifiable tallying function $\boldsymbol{D}$ such that $\forall x \in \boldsymbol{C}$, $\boldsymbol{D} \circ \phi \circ \pi \circ \sigma(x) = x$. The preparation may involve publishing commitments, keys, etc. depending on the particular $\boldsymbol{D}$. One can say that a sigma ballot encrypts a clear text vote x into a coded vote y and $\boldsymbol{D}$ decrypts y back to x. A sample $\boldsymbol{D}$ is described in section 5.

To check that $\forall x \in \boldsymbol{C}$, $\boldsymbol{D} \circ \phi \circ \pi \circ \sigma (x)=x$, a public auditor chooses a statistically significant number of ballots and asks the election authority for the information such that the equation $\boldsymbol{D} \circ \phi \circ \pi \circ \sigma (x)=x$ can be publicly checked. This is the very first step of the protocol and is done before Election Day, before ballots are printed.

The next step is to produce Sigma ballots and receipts, using one of the protocols described in section 3.

After the voter obtains her receipt, the following commitments are opened:

1. If the receipt contains the order of the candidates, the commitment to the entire function σ is opened.
2. If the receipt contains the position x of the marks, the commitment to $(x, \pi(x))$ is opened.
3. For the confirmation code x which is always on the receipt, the commitment $(x, \phi(x))$ is opened.

If a voter complains that she does not see the correct confirmation codes posted on the public bulletin board, she is asked to provide the confirmation codes that she thinks should be on the bulletin board. Then the election authority opens all commitments to x, $\forall x \in \pi(\boldsymbol{Z}_c)$. If the confirmation code provided by the voter is not among the opened ones, then the voter must be wrong. If it is among the revealed ones, and since the confirmation codes are difficult to simply guess, then, if a statistically significant fraction of voters provide confirmation codes that are among the committed ones, this becomes an indication of malfunction.

If the voter does not see her paper receipt correctly posted on the public bulletin board, i.e., the order of the candidates or the position at which the marks appear is not the same, then the voter can bring her paper receipt as irrefutable proof of malfeasance.

Anybody can inspect the bulletin board and check that the commitments are consistent with the posted receipts, i.e., with the order of the candidates or with the association between confirmation codes and the marked positions. Also, anyone can check the commitments to the confirmation codes themselves or the commitments to the association between confirmation codes to coded votes.

5 One way to produce the tally

Inspired by Scantegrity II [CD08], we briefly describe an example of a function ***D*** that allows everyone to check that all the receipts have been correctly tallied. This scheme is not a contribution of this paper, and it is presented only for completeness.

Let N be the number of ballots in an election and let c be the number of candidates on a ballot. Consider three tables (see Figure 4): table R contains coded votes, table T contains clear text votes that are countable by anyone and table D connecting R with T. R is a matrix with N rows and c columns, each row represents the coded votes of a ballot. R is a matrix with c rows and N columns, each row representing a candidate. An element (i, j) is either marked or not marked in R and T. A mark in T corresponds to a vote for a candidate. D is a set with N * c elements. Figure 4 gives an example of the three tables for an election with six ballots and two candidates.

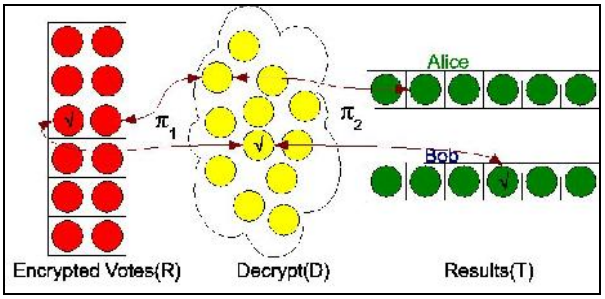


Figure 4: Pointer-based mixnet

The tables are connected by two permutations, π_1 and π_2. π_1 connects R with D: $D_k=R_{\pi 1(k)}$, where k is some canonical representation of (i, j), e.g., k=(c-1)*i+j. Similarly, π_2 connects D with T: $T_k=D_{\pi 2(k)}$.

The properties of the permutations may be formalized as follows: let π_1: $\boldsymbol{Z}_{n \times c} \rightarrow \boldsymbol{Z}_{n \times c}$ be bijective and let π_2: $\boldsymbol{Z}_{n \times c} \rightarrow \boldsymbol{Z}_{n \times c}$ be bijective such that no two coded votes belonging to the same ballot initially (in the same row in table R) are mapped to two elements belonging to the same candidate (the same row in table T):

$$\forall\ i,j,\ i \neq j \text{ having } [\ i / c\ ] = [j / c] \rightarrow [\pi_2(\pi_1(i)) / b] \neq [\pi_2(\pi_1(j)) / b] \qquad \text{Equation 1}$$

where [x] represents the greatest integer less or equal to x. The function ***D*** that provides a universally verifiable tally function is $\boldsymbol{D} = \pi_2 \circ \pi_1$.

Initially, the election authority publishes commitments to each mapping done by π_1 and π_2, along with the commitments needed for the Sigma ballots, including the commitments that tie in the confirmation coded to the coded vote (the indexes in the R table). To check the correctness of this step, an auditor can request some statistically significant number of ballots to have their commitments opened. When a cast ballot is received, the election authority opens the commitment that ties the confirmation code to the coded vote in the R table. After the polls close and the index in the R, D and T are marked, the final audit checks that one of the two properties hold, at random: $D_i=R_{\pi 1(i)}$ or $D_i=T_{\pi 1(i)}$ and that the properties of the two permutations π_1 and π_2 hold, i.e., it checks

that both π_1 and π_2 are injective functions and that Equation 1 holds for each of the revealed pairs of π_1 or π_2. Because the voting system cannot predict which permutation will be checked, a successful audit implies that the coded votes have been correctly transformed into clear text votes with high probability. Privacy is preserved, since no complete link is revealed from the R table to the T table, but only links from either R to D, or from D to T.

6 Conclusions

We have presented a new type of filled-in ballot which has confirmation codes like Scantegrity II and the order of the candidates permuted like Prêt à Voter. The advantages of Sigma ballots combine the ability to easily check that they have been correctly printed with the ability to file a complaint without the need for the voter to present physical evidence. At the same time, Sigma ballots solve some of the issues of Scantegrity II, such as adding marks after the ballots have been cast, or needing to create receipts by hand. Sigma ballots produce a "something you know" receipt to check the correct recording of the cast ballot and a "something you have" receipt to check the correctness of printing.

We described two ways in which Sigma ballots can be produced: using a DRE+VVPAT or using an optical scan Scantegrity II ballots. The DRE+VVPAT approach seems to be the most promising one, since it combines the advantages of having a robust and precise interface with the availability of hand countable paper ballots, and on top of that, the publicity verifiable tallying method.

Bibliography

[AR06] Adida, B, and R. Rivest. 2006. Scratch & vote. Self-contained paper-based cryptographic voting. In *WPES '06. Proceedings of the 5th ACM workshop on privacy in electronic society*, 29– 40. New York, NY, USA: ACM Press.

[AB09] Adida, B. et al. 2009. Electing a university president using open-audit voting. Analysis of real-world use of helios. In *Electronic voting technology workshop/workshop on trustworthy elections*. Usenix.

[CD04] Chaum, D. 2004. Secret-ballot receipts. True voter-verifiable elections. *IEEE Security and Privacy* January/February: 38–47.

[CRS05] Chaum, D., P. Y. A. Ryan, and S. Schneider. 2005. A practical voter-verifiable election scheme. In *ES-ORICS*, *volume 3679 of lecture notes in computer science*, ed. Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, 118–139. Springer (http://www.springerlink.com/content/ebrbl9kc81bhx98j/).

[CD08] Chaum, D. et al. 2008. End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *EVT'07. Proceedings of the USENIX/accurate electronic voting technology workshop*. USENIX Association.

[EA07] Essex, A. et al. 2007. Punchscan in practice. An e2e election case study. In *IAVoSS workshop on trustworthy elections (WOTE 2007)*. University of Ottawa, Canada.

[KJ07] Kelsey, J. et al. 2007. Some random attacks on paper-based e2e systems. http://kathrin.dagstuhl.de/files/Materials/07/07311/07311.KelseyJohn.Slides.pdf/. (accessed 17 November 2008).

[PH06] Popoveniuc, S., and B. Hosp. 2006. An introduction to PunchScan. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2006)*. Robinson College, Cambridge.

Session 6: E-Voting Experiences

Electronic Elections in a Politicized Polity

Thad Hall[1] and Leontine Loeber[2]

[1]Associate Professor of Political Science, University of Utah
260 S. Central Campus Drive, Room 252
Salt Lake City, UT 84112
USA

[2]University of Leiden, Netherlands
Professor Paul Scholtenlaan 48
1181 ME Amstelveen
The Netherlands

Abstract: Since the 2000 presidential elections, the evolution of electronic technologies in American elections–from voting machines to computerized voter registries–has occurred within the context of a highly partisan, polarized, and politicized environment. The decision about the type of voting systems to use within a given state has become especially political and these debates have affected the confidence and attitudes of voters toward various voting technologies. In the Netherlands, the debate even led to abolishing the use of all electronic technologies in elections. In this paper, we consider the evolution of voter confidence over this period and the evolution of the political debate that relates to electronic voting. We note that confidence in voting systems is affected by several factors, including race, partisanship, voting for a winning candidate, and the mode of voting (i.e., voting in person or voting via absentee ballot). During this time, certain factors, such as partisanship, have changed in importance based on previous election outcomes. On the issue of the importance of partisanship on confidence, we compare the United States and the Netherlands and the evaluation of electronic voting.

1 Introduction

A polity is a geographic area with a corresponding government. The term is also used to refer to a state or a lower level government such as a province, municipality or district. A polity can become politicized when different political factions appear. This may lead to changing policies with regard to electronic elections. A policy is a set of decisions to achieve a rational outcome. In this paper we look at different factors that may influence policies concerning electronic voting in politicized polities. The study of confidence in the electoral process–especially the process of counting ballots–in the United States has become a major field of research since the disputed 2000 presidential election. In that election, the decision regarding who won the race for president, between Al Gore and George Bush, became a tangled legal issue, largely because of the difficulties associated with determining how to count and recount ballots in the State of Florida. The decision of the United States Supreme Court in *Bush v. Gore* determined that recounts in the election would end, making George Bush the victor, but the controversies surrounding election administration and voting technologies continued. Throughout 2001 and 2002, several research groups and blue-ribbon commissions examined the elections in the United States and made recommendations that informed the passage of the Help America Vote Act (HAVA) of 2002 [VTP01, CF02]. Given that the most visible problem from the 2000 presidential election was the issue of how to count ballots, it is not surprising that the centerpiece of HAVA was providing funding to states to purchase modern voting technologies, with the intent of solving the vote-counting problem through the acquisition and implementation of new voting systems.

However, the contentiousness of the 2000 election was not just the result of the debate over the way votes were counted and the closeness of the election in the state of Florida. As many scholars have noted, the 2000 election occurred in a period when the American electorate had become increasingly polarized [AS08]. The highly politically engaged are especially polarized and there is evidence of strong partisan polarization in America as well. Liberals and conservatives, and Democrats and Republicans, view the political world quite differently; their issue preferences are highly bifurcated across an array of policy issues. In addition, the electorate is becoming divided geographically, with more states becoming uncompetitive and relatively few states serving as battlegrounds for electoral competition at the presidential level [AS08; Bi08]. These divisions in America have become much more pronounced than they were in the 1960s, with polarization increasing throughout the 1970s, 1980s, and 1990s.

One key issue for voting is how polarization and having a polarized electorate affects the confidence of voters in the voting process. Given the problems that existed in the 2000 election, it is reasonable to ask whether the partisan polarization–combined with issues with election administration–affects the willingness of losers to "consent" to the outcome of the election. The question of consent among losers is critical for the legitimacy of election administration because, although winners always find the election to have been fair, losers have to think and feel that the process that resulted in their loss was fair [ABB05]. This consent is needed not just from the candidates and parties; voters themselves must be confident that election administration is not being manipulated for partisan reasons.

In the Netherlands, electronic voting was introduced in 1966 and was for a long time no subject of debate. The confidence in the system was very high, which led to more and more municipalities making the choice for voting machines. During the municipal elections of 2006, 99% of the voters voted on a direct recording electronic (DRE) voting machine. In the summer of 2006, an action group called "We don't trust voting computers" was founded, which started a media campaign against the voting machines in use. This led to several debates in Parliament and ultimately to the abolishment of all forms of electronic voting. After the parliamentary elections of 2006, voters were asked whether they had confidence in different forms of electronic voting. This research, done in the National Voters Study 2006, is the first major study done in the Netherlands concerning voter confidence.

In the United States, there has been an effort since 2004 by political scientists to measure voter confidence in the electoral process. This effort has examined confidence generally in the electoral process, but also with specific methods of voting, such as electronic voting or voting with machine-counted paper ballots. In this paper, we review the findings in this literature and present new analyses that show how Americans remain divided in their confidence levels in the voting process generally and with specific voting technologies. We discuss how a simple measure of confidence can be used to evaluate the attitudes of voters and election officials in various aspects of the electoral process. We then consider how voter confidence has changed over time in the electoral process and how partisanship, ideology, and the voting technology used all affect the confidence of individuals participating in the electoral process.

The American context for studying voter confidence and considering the effects of voting technologies on confidence has occurred in the shadow of the 2000 presidential election controversy. In order to disentangle the issue of voter confidence and voting technology, we compare the findings of the United States with results from the Netherlands. There, there was a great controversy over the security and efficacy of electronic voting in 2008, which led the government to disallow the use of these machines in elections in the Netherlands. We can compare confidence in the American context with the Netherlands to see how partisanship and attitudes toward voting technology are treated in both contexts. We can then see how the American experience may be unique in some ways, but not others, regarding voter confidence.

2 Measuring Confidence in the Electoral Process

Although discussions of voter confidence have existed in the United States for some time–the term "confidence" was used in the report of the National Commission on Federal Election Reform (Carter and Ford 2002)–the systematic measurement of voter confidence in the voting process has been a more recent phenomenon. In 2004, Alvarez and Hall conducted one of the first studies to use what has become a standard voter confidence question. The question they used was, "How confident are you that your vote was [or will be] counted as intended in [the election]?" with the response options "very confident," "somewhat confident," "not too confident," or "not at all confident." As

Alvarez, Hall, and Llewellyn (2008, 755) discuss, this measure "define[s] trust in the electoral process as the confidence that the voters have that their ballot was counted as intended." As Gronke and Hicks (2009) note, several scholars have used voter confidence as a metric for studying voter attitudes toward election reforms [Ha08] and Stewart (2009) has referred to this voter confidence metric as "a summary judgments of the voting experience."

Scholars have also broadened this concept in a small number of surveys to ask voters not just "how confident are you that *your vote* will be counted as intended," but also "how confident are you that *all votes in your county* will be counted as intended" and "how confident are you that *all votes in your state* will be counted as intended" [AAH09; AS07]. These broader measures are designed to determine if voters have different levels of confidence across varying levels of government–their vote, votes administered by a process in their county, and votes administered by various processes and various officials across the state–and various levels of abstraction in the process (your vote, votes in a county, votes in the state).

A key question that has emerged regarding the use of this metric is whether the metric is merely a reflection of the respondent's trust in government or the respondent's expectation of their candidate winning the election. Alvarez, Hall, and Llewellyn (2008) make the claim that there is no *a priori* reason to think that vote confidence and trust in government are the same. They argue, "Voters may not possess confidence in the voting technology used to cast a ballot, but trust their elected officials completely. Alternatively, voters may believe that the electoral process is fair and accurate, but simultaneously hold the belief that all politicians are crooks" [AHL08, 755]. They put the question of voter confidence within the literature on trust, but note how the two concepts are different.

Recently, Atkeson, Alvarez, and Hall (2009) and Gronke and Hicks (2009) independently tested the validity of this construct, explicitly examining whether voter confidence and voter trust are truly distinct concepts. Atkeson et al. (2009) compare three types of voter confidence–personal vote, the votes in a county, and votes in a state–with a measure of trust in government and a measure of political efficacy. They find that the confidence questions load differently in a principal-component analysis compared to the trust and efficacy questions; they are not part of the same dimension. In addition, trust, efficacy, and confidence have different correlation relationships; the confidence questions are highly inter-correlated, but these questions in turn are not as correlated with either trust or efficacy. Importantly, when used as dependent variables in a regression model, different factors predict voter confidence when compared to either efficacy or trust. For the confidence questions, a voter's experience voting affects voter confidence, but is unrelated to either trust in government or efficacy.

Gronke and Hicks (2009) use a different methodology to come to the same result. Specifically, they run a series of regression analyses to determine if voter confidence is explained by trust in government, confidence in social or political institutions, current economic-political factors, or by election administration experiential factors. They determine that, although trust in government and confidence in election officials do help

to shape voter confidence, election experience is a strong predictor as well. If voter confidence were merely another measure of trust in government, these other factors would be washed out by the high correlation between trust and confidence. This adds weight to arguments that the voter confidence metric is a sound one to use as a "summary measure" for determining a voter's confidence in the electoral process, at least in the American context.

In the Netherlands, the study of voter confidence has been done in the context of the National Election Survey. This survey is conducted before, during, and after elections for Parliament. It studies a wide range of subjects and contains nearly 700 questions. Different questions are asked before and after the election. During the Parliamentary Elections of 2006 a series of questions was added to the survey conducted after the election on voter confidence, both in the outcome of the election in general and in different voting methods. These questions were asked in light of the discussion on voting machines. Around 2800 participants answered these questions.[1]

3 Experiential Influences on Voter Confidence

Research on voter confidence has generally focused on three sets of attributes that affect confidence in the voting process. First, there have been studies examining the way in which the voting experience–especially during in-person election-day voting–affects voter confidence [e.g., AAB09; CMM08; GH09; Ha09; HMP09]. These studies have found that voter confidence is affected by voter experiences at the polls. Voter confidence is sensitive to the experience that voters have with their poll workers; poll workers that are not seen as competent can negatively affect voter confidence. This is not surprising, given the important role that poll workers play in ensuring that votes are counted and counted accurately.

Second, there have been relatively consistent findings that voter confidence varies across modes of voting. This finding has been made by numerous scholars and the one consistency of these findings is that voter confidence is predicated on the mode by which voters cast their ballot [e.g., AH04, AH08A, AHL08, AHL09, AS07, AAH07, Ha09, St09, AAB09]. In the American context, there are three modes by which voters can cast their ballots, although these laws do vary by state [AAB09]; voters can cast a ballot (1) in person in a polling place on Election Day, (2) in person in a polling place during a period prior to Election Day (often the two weeks prior) in an "early voting" location, or (3) remotely, using a paper ballot that is mailed back to their election office (absentee or postal voting).[2] In the Netherlands, voters can vote in person in a polling place on Election Day. However, unlike in the United States, Dutch voters cannot vote absentee. They can give a proxy vote to a voter of their choice. A proxy vote can be given by a

[1] For more information about the survey and its methodology, see http://www.dpes.nl/, last accessed on 10 May 2010.

[2] The rules for absentee voting vary by country and can (as in the case of the United States) vary by subdivision within the state. In the United States, absentee voting occurs by the election official mailing the ballot to the voter and the voter mailing the ballot back. By contrast, in Estonia absentee voting is done using the Internet and in the Dutch case, the voters choose someone to cast a ballot for them.

voter who cannot vote in person at the polling station on Election Day to any other voter. The voter who receives the proxy vote is allowed to cast the vote for the other person. A voter can only cast proxy votes for two voters. Even though the system allows voters who cannot vote in person to use their vote, they have no guarantee that the person they give their proxy vote to will cast their vote as intended. Voters who live abroad can vote either by postal ballot or, in the 2006 elections, by Internet. For all voting methods, it is possible to cast a blank vote.

	Mode of Voting		
Confidence	In Person Election Day	In Person Early	Absentee
Not Confident	1.92%	1.62%	2.52%
Not too Confident	3.02%	2.61%	5.63%
Somewhat Confident	20.16%	22.87%	31.76%
Very Confident	74.91%	72.90%	60.09%
	Mode of Voting		
Trust in Elections	Proxy Voter	Voted In Person	
Very Much	31.56%	31.17%	
Much	49.78%	49.87%	
Not Too Much or Too Little	12.89%	13.29%	
Little	3.11%	4.89%	
Very Little	2.67%	0.77%	

Table 1: Confidence and Trust by Vote Mode

The research on voter confidence shows that voters who cast ballots using absentee voting are much less confident than voters who vote in-person, either early or on Election Day. In the top half of Table 1, we show the confidence of voters across various vote modes using data from the *2008 Survey of the Performance of American Elections* [AAB09]. These data illustrate the large gap in confidence between in-person and absentee voters. Absentee voters have many potential reasons for being less confident that their vote will be counted accurately, which may arise largely because these voters are less confident that their vote will be counted at all. In absentee voting, voters typically surrender their ballots to a third party–a postal service–and typically have to guess as to whether their ballot was received in the time frame required for ballots to be counted. These concerns are well founded; a small but significant percentage of ballots are rejected because they are received at the local election office after the deadline for including such ballots in the vote count [AHS08]. Even among ballots that were received in a timely manner, another cluster of ballots contains errors that result in the ballots being disqualified and not included in the ballots counted. Even after this hurdle is eclipsed, the vote on the ballot may still have an error that results in the vote not being counted for a given race.

In the bottom half of Table 1, we show data on voter confidence that uses a slightly different question than the one used in the American context. Here, we examine trust in the elections process generally by voting mode in the Dutch context. Here, we see that there are no significant differences in trust between voters who cast a vote in person and voters who gave a proxy vote. Both groups have the same levels of trust in the voting process.

Finally, there has been research on voter confidence and how it is related to the voting technology the individual used to cast her ballot [AH04, AHL08, AL08, AS07, HNH08, St09]. In these studies, the primary analysis has been whether voting technologies affect voter confidence. The findings of these studies have been relatively consistent; in the United States, voters using DREs tend to be less confident than voters who vote on paper ballots. For example, Alvarez, Hall, and Llewellyn (2008) found that voting on a DRE lowered the predicted probability that an individual would have their vote counted accurately by sixteen percentage points compared to a voter who voted using a paper ballot. Interestingly, this decline in confidence is the same as the decline in confidence for individuals who vote absentee. The confidence was even lower if an individual had low levels of trust in electronic voting generally.

In his study of the 2008 election, Stewart (2009) extended the work of Alvarez, Hall, and Llewellyn to determine if their results held in the 2008 election. Using a variety of statistical analyses, including ordered probit and ordinary least squares regressions (with state fixed effects and without), he found that voting technology was an important part of the confidence equation. Specifically, voters who cast ballots using electronic voting technologies were less confident than voters who cast ballots using optical scan voting. In addition, important for the discussion of voter confidence and polarization in the next section, Stewart found that liberal voters who used DREs were much less confident than were other voters who used DREs. In fact, conservative voters who use DREs are especially confident that their vote is counted accurately.

In the Netherlands however, in the 2006 Parliamentary elections, more voters expressed confidence in the DREs than in paper ballot voting; 80% of the voters expressed high levels of confidence in voting by DRE but the confidence level for paper ballot voting was 74%. When asked what type of voting method a voter preferred, DRE or paper ballot, 50% of the voters preferred voting by DRE and only 14% paper ballots. The 2006 election was the last election before the decision to terminate use of DREs in the Netherlands. During the 2006 election, out of around 400 municipalities, only 35 municipalities used paper ballot voting, the rest used DREs made by the Nedap Company.

4 Voter Confidence and Political Polarization in the United States

The fact that there are variations in confidence across voting technologies and voting modes–early, absentee, and Election Day–leads to questions regarding the political and ideological factors that also may affect voter confidence. There is a strong rationale for thinking that liberals and Democrats would be less confident overall compared to conservatives and Republicans, as well as thinking that liberals and Democrats would be less confident in electronic voting. The issue of overall confidence in this political and ideological context can be explained as resulting from two factors. First, Democrats were on the losing end of the 2000, 2002, and 2004 elections–elections that were generally very close and very polarizing. The close and controversial aspects of the 2000 election in Florida and the 2004 presidential election in Ohio–where both Secretaries of State were Republicans who had endorsed President Bush–led many Democrats to view these election as being one where partisan decision making had made the playing field unfair [AH08a].

Second, there were linkages made between the outcomes of these elections and the use of electronic voting. The concerns about electronic voting arose because of research that found problems associated with the Diebold DRE) voting machines that were used in several states, including Georgia and Maryland [KSR04]. These technical concerns became and remain a contentious source of debate, which centers primarily on whether DREs can be secured using standard methods for securing election materials through chain of custody procedures (AH08b).

These technical concerns became politicized when various advocates attempted to make links between electronic voting and pro-Republican election outcomes, starting with claims that the election in the state of Georgia in 2002 was potentially fraudulent. As Alvarez and Katz (2008) note,

> The allegations and concerns about the potential for election fraud in the trial use of these "touchscreen" voting systems in Georgia's 2002 election only worsened when the chairman and chief executive of Diebold, Inc., the corporation that produced the "touchscreen" voting machines used in Georgia was quoted in a Republican fundraising letter that he was "committed to helping Ohio deliver its electoral votes to the president next year."[3]

Alvarez and Katz (2008) review the claims of irregular outcomes in the 2002 senatorial and gubernatorial elections in Georgia—which introduced DREs statewide the same year—and use statistical analyses to refute these claims of fraud associated with electronic voting. However, questions continued to be raised about the accuracy and validity of elections conducted using DREs through the 2006 elections, as various issues have come up in jurisdictions that use electronic voting. Ironically, the same polarization has not occurred with similar problems with electronically counted paper ballots

[3] Schwartz, John. 2004. Executive calls vote-machine letter an error. *New York Times*, May 12, section A, column 6, page 19.

[AH08a]. The debate over electronic voting has also failed to consider the important issue of usability and effective interaction between the voter and the voting technology– the issue that was the original concern of reformers after the 2000 presidential election. Work in this area has examined the usability of various voting equipment and the evaluation that voters have of these technologies [HNH08]. These data show that voters have varying attitudes toward specific voting technologies and that it is incorrect to view all electronic voting as being the same. Voters differentiate between various types of DREs and between DREs and paper ballots in ways that are much more subtle than would normally be thought.

We see evidence of the difference in attitudes toward electronic voting among political partisans in survey data where voters are asked the following: "I'm going to read you some statements about electronic voting and want to know whether you agree or disagree with each statement, or if you have no opinion. 'Electronic voting systems increase the potential for fraud.'"[4] Table 2 shows data for this question from surveys conducted 25–29 August 2004, 9–15 March 2005, and 26–31October 2006 by International Communications Research

		Agree	Disagree	No Opinion
Oct-06	Republican	32	40	26
	Democrat	46	21	29
	Independent	39	21	37
Mar-05	Republican	33	37	28
	Democrat	47	23	28
	Independent	36	31	32
Aug-04	Republican	34	32	30
	Democrat	40	23	35
	Independent	40	31	29

Table 2: Electronic Voting and the Potential for Fraud

In each case, we see that Democrats are more likely to think that electronic voting increases the potential for fraud compared to Republicans and that the Democrat/Republican gap on this issue widens from six percentage points before the 2004 election to thirteen points after the 2004 election. This widening gap comes from Democrats becoming more sure that electronic voting increases the potential for fraud; the attitudes of Republicans stays the same on the agree side of the question, but five percentage points more Republicans disagree with this statement between the three surveys.[5] The data from the 2006 wave is shown in the top third of the table; it closely

[4] A detailed discussion of these survey data and the methodology for their collection can be found in Alvarez and Hall 2008a and Alvarez, Hall, and Llewellyn 2008.

[5] The survey marginals presented in Figure 3 do not show the "don't know/no response" category. In the first survey, 4.6 percent of Republicans answered, "don't know" compared to 1.6 percent of Democrats. In the second wave, Republicans and Democrats were almost equal in this category (1.9 percent Republicans, 2.3 percent Democrats).

mirrors the 2005 survey data and suggests a relative stability in attitudes about electronic voting and the likelihood of it increasing the potential for fraud during this period.

There are also differences between Democrats and Republicans in their confidence that their vote will be counted accurately. If we look at data from before the 2006 election in the three waves of surveys, we see that there are marked differences between Democrats and Republicans who are very confident–Republicans are much more confident than Democrats are that their votes will be accurately counted. Prior to the 2006 election, we see that, even combining the very confident and somewhat confident categories for Democrats, more Republicans are very confident than Democrats are very or somewhat confident.

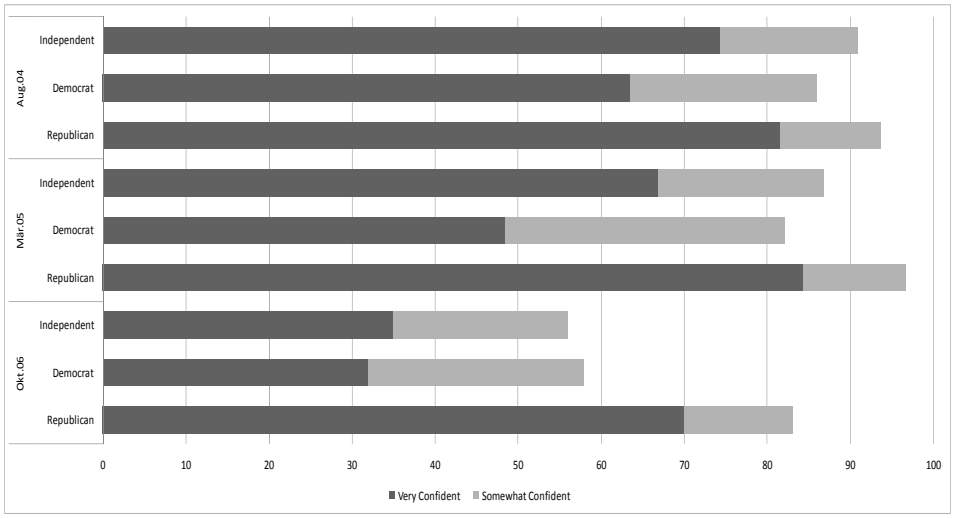


Figure 1: Voter Confidence by Party Affiliation

If we consider the context of the 2000 and 2004 elections–where Democrats lost close elections for the presidency and suffered losses in the Senate in 2002–it is not surprising that Democrats expressed little confidence in the electoral process. For many, it was likely easier to blame the electoral process than blame voters and the candidates for these losses. However, in 2006 and 2008, the Democrats were on the winning side of the elections. In 2006, Democrats nationally recaptured control of the Congress and, in 2008, they recaptured control of the Presidency. So how did these wins affect voter confidence?

We can examine this by using data from the Cooperative Congressional Election Study (CCES), which is a national survey conducted by Polimetrix in which individuals were surveyed before and after the 2006 congressional elections and the 2008 presidential elections.[6] Before the election, individuals were asked about their confidence that their

[6] For more information about the survey and its methodology, see http://web.mit.edu/polisci/portl/cces/index.html (last accessed 1 June 2009).

vote ***would be*** counted accurately, and after the election, they were asked their confidence that their vote ***was*** counted accurately. Figure 2 shows the pre- and post-election confidence for Democrats and Republicans after each of these elections. In 2006, we see that the percentage of Democrats who were very confident doubled between the pre- and post-election surveys and the percentages of Democrats who stated being not too confident or not at all confident declined by half as well. Republicans–who were much more confident to begin with–saw little change in their confidence in the pre- to post-election surveys. In 2008, we see a similar pattern; Republicans have a relatively stable level of confidence between the pre- and post-election surveys and Democrats have a sharp increase in the percentage reporting being very confident in the post-election survey compared to the pre-election survey.

As Alvarez, Hall, and Llewellyn (2009a, 2009b) have argued, this result can be viewed as a form of "winner's effect" that is conditional on an election outcome being different from the outcome that was expected for one of the parties. In the case of the 2006 and 2008 elections, Republicans expressed relatively high levels of confidence in the system before the election, but were not surprised by losing, given the level of polling on these elections and the amount of conservative punditry that had predicted–even welcomed the idea of–Republican losses. Democrats, on the other hand, had a more "believe it when I see it" attitude, which led them to have lower baseline levels of confidence pre-election and a relatively strong surge in overall confidence after the election.

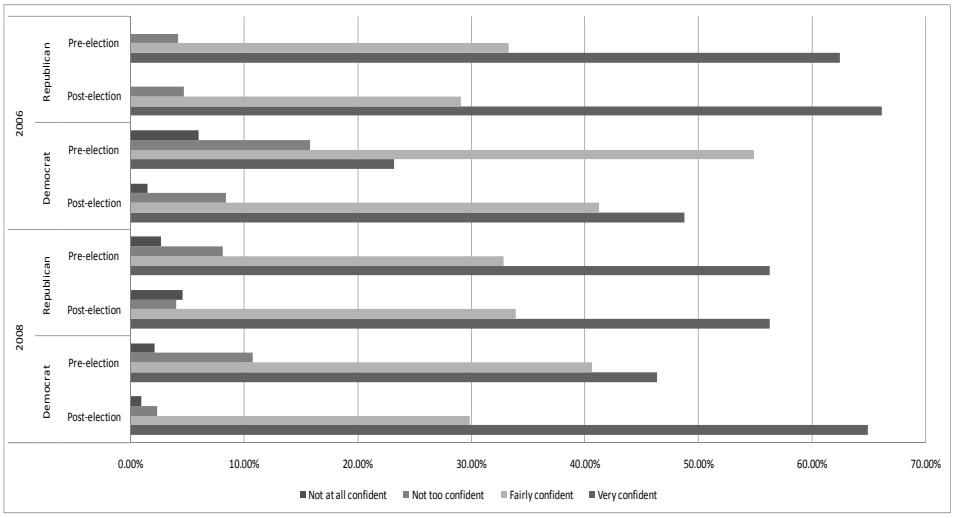


Figure 2: Pre- and Post-Election Confidence 2006 and 2008

In their work on a winner's effect in the 2006 elections, Alvarez, Hall, and Llewellyn (2009a) found that, in the pre-election voter confidence model, Democratic voters, and Independent voters, had significantly lower levels of confidence compared to Republicans. Specifically, the first differences in an ordered logit model show that "hypothetically changing the voter's party identification from Republican to Independent decreases the likelihood of a very confident response by 21 percentage points and from Republican to Democrat lowers confidence by 28 percentage points." They also found

that individuals who lived in an area that the respondent felt was not dominated by one political party was more confident, pre-electoral confidence may be increased through a belief in the existence of a politically balanced or non-partisan local government [AHL09a].

By contrast, they found that post-election voter confidence was driven by both partisan and election administration factors. There was a winner's effect–Democrats did have a marked increase in confidence after the election. In addition, voters who think that there is congruence between their party identification and the party that controls the local government are significantly more likely to be confident compared to voters who have incongruence. This finding supports previous research [AS07] regarding the link between confidence and local government politics. The post-election voter confidence was also affected by the voting technology the voter used. Specifically, voters who used electronic voting were significant less confident than were voters who cast ballots using paper ballots. The negative effects of electronic voting, however, were made up for if voters voted on an electronic voting machine that had a paper audit trail (PAT) that allowed the voter to review a printed copy of their ballot before casting their electronic vote. In fact, voting on an electronic voting machine with a PAT made voters 14 percentage points more likely to be very confident compared to paper ballot voters [AHL08].

Alvarez, Hall, and Llewellyn (2009b) have also examined voter confidence in partisan primary elections, specifically the "Super Tuesday" presidential primaries held on 5 February 2008. These primary elections are interesting because they bring out the most committed partisan voters, who may have different views about the voting process compared to more casual voters. However, they find that the same factors that have been identified previously–a partisan difference in confidence between Democrats and Republicans (Republican primary voters have a higher base level of confidence compared to Democrats), lower confidence among absentee voters, and a "winner's effect" (voters in a primary who voted for a winner are more confident than those who voted for a loser)–all are significant in primary elections as well.

5 Voter Confidence and Political Polarization in the Netherlands

Because we only have data on voter confidence in the Netherlands for one election, it is not possible to see whether there are changes in voter confidence within supporters of the same party over time. It is however possible because of the multi-party system to look at the difference in voter confidence between voters of several parties, some of which were winners in the 2006 elections and some of which were losers. However, because of the Dutch proportional representation system coupled with coalition government, even parties that lose seats can still end up in government. In 2006, for example, this happened with the Labor Party (PvdA). Winning or losing in the Netherlands is therefore more relative than in the US. In the elections of 2006, the big winners were the Socialist Party (SP), the ChristenUnie, the Party for Animals (Partij voor de Dieren), and the party led by Wilders (PVV). Big losers were the Labor Party (PvdA), the Liberals (VVD), the Democrats 66 (D66), and the former party of Fortuyn (LPF).

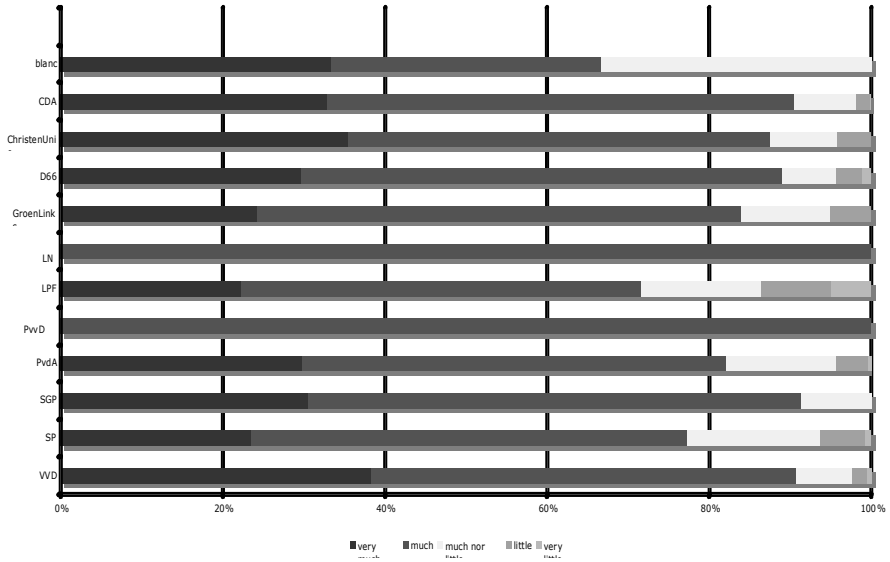


Figure 3a: Confidence in Voting machines

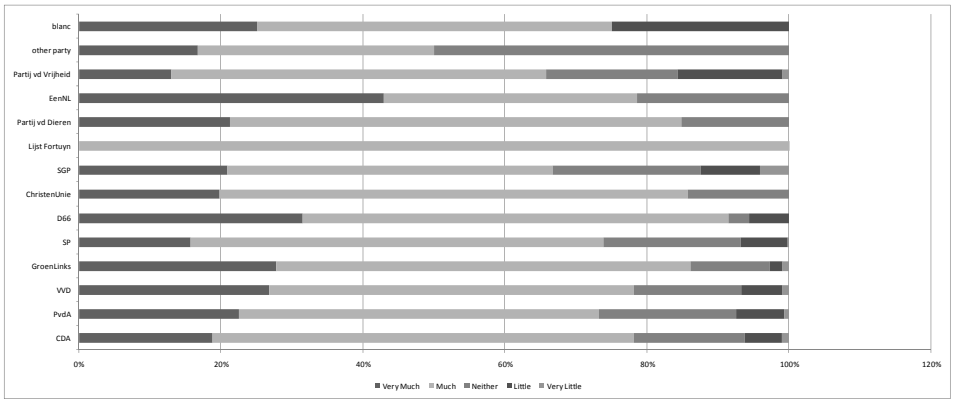


Figure 3b: Confidence in Paper Ballots

Figure 3a shows the confidence level in voting by voting machine of the voters of all the parties. In general, the trust in voting machines is very high, both with voters of parties that won compared to 2003 and parties that lost. One party that was actually a winner, the Socialist Party shows lower levels of trust. Two losing parties, the Liberals and the LPF have high levels of trust, compared to the other parties. The only voters that seem to have relatively low levels of trust in the DREs are the voters who voted blank. The same picture appears when looking at confidence levels with regard to paper ballot voting, as shown in Figure 3b. Again, one of the winning parties, the SP shows lower levels of confidence. The LPF, which lost all its seats, has a high level of trust. These figures do suggest that there is no winner or loser effect on voter trust in voting technology apparent in Dutch elections.

6 Reforms and Voting Technology: Reforms in a Polarized Electorate

The partisan differences that exist in voting technology in the United States may continue into the future, given the polarized views of Americans and the fact that Americans are "well sorted" both ideologically and geographically [e.g., AS08, Bi08]. This sorting makes politics in the United States self-reinforcing; individuals tend to be involved in self-referential worlds, interacting primarily with individuals who share their views. The debate over election fraud in the United States, for example, has a strong partisan bent as do debates over making voter registration and voting easier [AAB09, AHH08]. Given this partisan dynamic, how does the future debate over electronic voting look going into the future?

We can begin to see the potential future debate over electronic voting in recent survey data that asked 32,800 individuals who participated in the 2008 CCES survey conducted by Polimetrix. The survey asked individuals the following question: "States have tried many new ways to run elections in recent years. Do you support or oppose any of the following ways of voting or conducting elections in your state?" One reform the individuals were asked about was "Allow absentee voting over the Internet." Respondents were given the following response options: "Support," "Oppose," and "Not Sure."[7] Given the movement toward Internet voting that is currently either ongoing or under consideration across western countries, it is interesting to consider the attitudes of Americans toward these reforms and how the partisan nature of the debate over this reform might shape up.[8]

In Figure 4, we see that overall support for Internet voting in the United States is not tremendously high; 31.0 percent support Internet voting, 46.9 percent oppose this reform, and 22.1 percent are undecided. However, there are clear differences in attitudes between Democrats, Republicans, and Independents and between younger and older voters on this issue. First, Republicans are much more opposed to Internet voting than are Democrats. Only 20 percent of Republicans support the idea of Internet voting and 65.2 percent of Republicans oppose it. By contrast, Democrats have a more diverse set of viewpoints and are more undecided on it; 37.4 percent of Democrats support Internet voting and a roughly equal percentage (38.7 percent) of Democrats oppose it. In addition, almost 24 percent of Democrats are undecided about Internet voting compared to only 14.9 percent of Democrats. There are also differences in attitudes toward these reforms vary across age cohorts as well. Younger individuals have more positive views toward Internet voting than do older individuals, who are more negatively inclined toward this reform.

[7] Individuals could also skip the question. There were 26,066 valid responses to the survey question. The data in Figure 6 have 26,066 as the total number of cases analyzed, except for the partisan question, where individuals who did not state a party identification were excluded. For that table, 23,330 is the denominator.

[8] For a review of these reforms, see AH04, AH08a, MT04, TM05, TSB07.

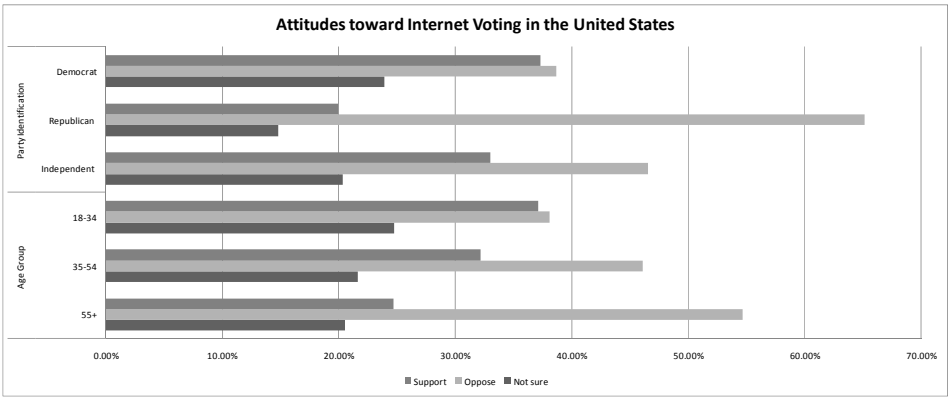


Figure 4: Internet Voting Attitudes in the United States

These partisan differences are not surprising, given that Democrats have used Internet voting in primary elections more than have Republicans, including the 2000 Arizona Democratic Presidential primary elections, the 2004 Michigan Presidential caucus, and the 2008 Presidential primary held by overseas voters. In addition, work internationally has shown differences in attitudes and in the use of Internet voting, especially in Estonia, across age groups. The key question is whether this reform will become one that has a partisan component, like the debate over electronic voting does in the United States, or whether Internet voting will be a reform that is debated without partisan suspicions. In Table 4, we see that there is not strong support for Internet voting in the Netherlands either.

Trust in Internet Voting	
Very Much	4,3%
Much	27,3%
Not Too Much or Too Little	21,2%
Little	33,7%
Very Little	13,4%

Table 4: Trust in Internet Voting

In the Netherlands, the debate on the use of voting technology led to an abandonment of all electronic forms of voting [JP09, Lo08]. These decisions were made after the 2006 parliamentary elections. Almost all parties in Parliament, whether they won or lost seats during this election, supported the return to paper ballot voting. This is remarkable, since most voters did express a higher trust in voting machines then in paper ballots as shown in Figure 5.

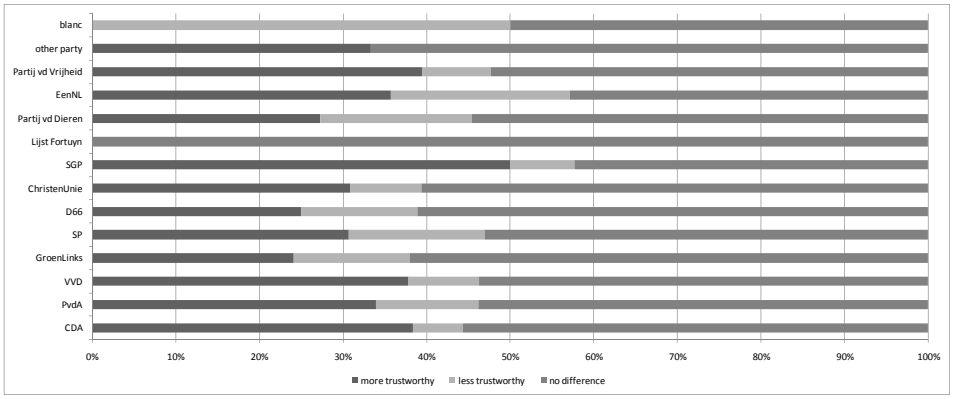


Figure 5: Trustworthiness of Voting Machine Compared to Paper Ballot

After the municipal elections of March 2010, the question whether or not to use electronic voting again became a topic of debate. During these elections, in which everybody voted with paper ballot, the results of the count were subject of discussion in a number of municipalities. There were problems with the proxy votes, in some cases two people were in the voting booth together and the votes were not always counted correctly.[9] Fifteen municipalities, including Rotterdam, the second largest city in the Netherlands, decided to do a recount of all the votes. This led to some cases of a seat being awarded to a different party. Parties that felt they had been 'cheated' out of seats raised the issue of trustworthiness. Some parties even demanded a revote. In Rotterdam, the two biggest parties, the PvdA and a local party, Leefbaar Rotterdam, achieved the same number of seats. Since by custom, the largest party is the first to try to form a coalition to govern, the exact number of votes that either party received became of importance. The PvdA had the most votes. Leefbaar claimed that a lot of the poll workers in Rotterdam were supporters of the PvdA and that this had helped them to become the biggest.[10] After the recount, which was done by different people and under scrutiny of the parties and the press, the PvdA still received the most votes.[11]

The municipal elections did show a more politicized debate on the use of certain voting techniques. The abandonment of the voting machines apparently did not mean that the same pathologies did not occur. On the contrary, where the use of voting machines had not raised issues on politicization of the voting process, with the paper ballot elections, there were politicized recounts. The security of the proxy voting system was questioned and issues were raised with regard to the accuracy of the results when paper ballots are used. This led to a strong call from the poll workers and the local election boards to return to a form of electronic voting. So far however, the government has stated that they have no intentions to do so.[12] Parliament has agreed to this course of action. Apparently,

[9] http://www.nd.nl/dossiers/politiek/gemeenteraadsverkiezingen-2010 (in Dutch only, May 23, 2010).
[10] http://www.deweekkrant.nl/pages.php?page=1112223 (in Dutch only, accessed May 23, 2010).
[11] http://www.ad.nl/ad/nl/1038/Rotterdam/article/detail/469496/2010/03/12/Hertelling-Rotterdam-PvdA-blijft-grootste-partij.dhtml (in Dutch only, accessed May 23, 2010).
[12] http://www.telegraaf.nl/binnenland/6223820/__Rood_potlood_niet_ter_discussie__.html (in Dutch only, accessed May 23, 2010).

the decisions made by government and parliament in 2007 and 2010 were not solely based on confidence in electronic voting, but also on other factors. Because electronic voting was in the past uncontroversial in the Netherlands, until now, there are hardly any studies that have focused on the motives of political parties to favor certain types of voting technology. More research is therefore needed to find out what motivated parties to abandon electronic voting.

7 Conclusions and Implications

Voter confidence in election results is of the utmost importance for the legitimacy of the chosen legislators. When the trustworthiness of the techniques and methods that are used during the elections become subject of a debate, this can have a negative impact on the confidence of voters. Voters or NGOs can raise the question of trustworthiness, as was the case in the Netherlands, but losing candidates can also be tempted to use the voting system as a scapegoat, as seems to happen in the United States and even in the 2010 municipal elections in the Netherlands. In the United States, the 2000 election raised critical questions about the performance of the nation's voting system and these questions have continued to resonate through the polity. Most troubling, they are creating questions among some voters about the security and accuracy of various voting technologies. These concerns have polarized characteristics in some cases, especially in regards to voting modes–voters tend to be less confident in by-mail voting compared to in-person voting–and across voting technologies, with liberals and Democrats less confident in DREs compared to conservatives and Republicans. In controversial elections, such as in 2000, 2002, 2004, and in certain specific races in 2006, voting technology has been the focus of media and political scrutiny, used to explain election losses and to question the voting process.

In the United States, one reason why confidence is so important is that losers are just that, losers. There is no proportional representation in Congress or in the Executive, so voting for a losing candidate can mean that your preferences will not be represented in the political debate. Obviously, there are people who vote for losing candidates, but the party they support may control the Congress or one chamber therein. However, in proportional systems, a voter's party can finish third or fourth and still get a plum portfolio in a coalition government. In the American context, losing can be a more bitter experience. The evidence points toward a clear loser effect on confidence in voting technology.

The Dutch case seems to support this thesis. In the proportional system that is used in the Netherlands, losing parties can be part of government. The data from the 2006 elections shows that the level of voter confidence in voting technology is not noticeably influenced by the fact of whether or not the party a person voted for won or lost in the elections. There are differences between parties in the level of voter confidence, but more research is needed to find what factors cause this. The March 2010 elections did show an increasing politicization of the debate on voting techniques. It remains to be seen whether or not this trend will continue.

As electronic voting technology use expands, debates over its efficacy have expanded as well. The Dutch experience with electronic voting is a case in point, where electronic voting technologies came under sharp scrutiny and were eventually removed from use [Lo08]. In the Netherlands, the advocates and opponents of electronic voting were not divided on party lines. Neither were they following the preferences of the voters, since these voters even expressed more confidence in electronic voting than in paper ballot voting. However, if such debates become politicized, they can undermine trust and confidence in the voting process. As advocates and politicians link to address concerns about certain voting technologies, the pro and con sides of these debates can take on partisan dimensions, with one party or set of parties associated with liking or disliking one voting technology or mode of voting over another. In the American context, such linkage has occurred with electronic voting, as Democrats and liberals associate DREs with pro-Republican interests. After the 2008 elections, these positions may have shifted. If positions in the debate on the use of electronic voting depend solely on partisan dimensions, other objectives of electronic voting, such as the improvement of voter accessibility may be overlooked. Other countries (e.g., Estonia) have much clearer core ideals about the efficacy of electronic voting and these core ideals make confidence in the system higher [TSB07]. The American example is a cautionary one; when voting technologies are politicized, they can undermine confidence in the voting process.

Bibliography

[AS08] Abramowitz, A. I., and K. L. Saunders. 2008. Is polarization a myth? *Journal of Politics* 70 (2): 542–555.

[AH04] Alvarez, R. M., and T. E. Hall. 2004. *American attitudes about electronic voting.* Salt Lake City: Center for Public Policy and Administration at the University of Utah.

[AH08b] Alvarez, R. M., and T. E. Hall. 2008b. Building secure and transparent elections through standard operating procedures. *Public Administration Review* Sept/Oct.: 827–837.

[AH06] Alvarez, R. M., and T. E. Hall. 2006. Controlling democracy: The principal-agent problems in election administration. *Policy Studies Journal* 34 (4): 491–510.

[AH08B] Alvarez, R. M., and T. E. Hall. 2008a. *Electronic elections: The perils and promise of digital democracy.* Princeton, NJ: Princeton University Press.

[AH04] Alvarez, R. M., and T. E. Hall. 2004. *Point, click, and vote: The future of Internet voting.* Washington, DC: Brookings Institution Press.

[AAB09] Alvarez, R. M., S. Ansolabehere, A. Berinsky, G. Lenz, C. Stewart III, et al. 2009. *2008 survey of the performance of American elections.* Boston/Pasadena: Caltech/MIT Voting Technology Project.

[AHL08] Alvarez, R. M., T. E. Hall, and M. Llewellyn. 2008. Are Americans confident their ballots are counted? *Journal of Politics* 70 (3): 754–766.

[AHL09a] Alvarez, R. M., T. E. Hall, and M. Llewellyn. 2009a. *The winner's effect. Voter confidence before and after the 2006 elections.* Working Paper. Pasadena, CA. http://vote.caltech.edu/.

[AHL09b] Alvarez, R. M., T. E. Hall, and M. Llewellyn 2009b. Voter confidence in partisan primary elections. Working Paper. Pasadena, CA. California Institute of Technology.

[AHS08] Alvarez, R. M., T. E. Hall, and B. Sinclair. 2008. Whose absentee votes are returned and counted: The variety and use of absentee ballots in California. *Electoral Studies*. 27: 673-683.

[ABB05] Anderson, C. J., A. Blais, S. Bowler, T. Donovan, O. and Listhaug. 2005. *Losers' consent: Elections and democratic legitimacy.* Oxford: Oxford University Press.

[AS05] Ansolabehere, S., and C. Stewart III. 2005. Residual votes attributable to technology. *Journal of Politics* 67 (2): 365–389.

[AS07] Atkeson, L. R., and K. L. Saunders. 2007. Voter confidence: A local matter? *PS: Political Science and Politics* 40: 655-660.

[AAH09] Atkeson, L. R., R. M. Alvarez, and T. E. Hall. 2009. Government trust and voter confidence: How similar are they? Paper presented at the annual meeting of the *Midwest Political Science Association,* Chicago, IL: April 2-5, 2009.

[AAH07] Atkeson, L. R., R. M. Alvarez, and T. E. Hall. 2007. *The New Mexico election administration report: The 2006 November general election.* Albuquerque: University of New Mexico.

[Bi08] Bishop, B. 2008. *The big sort.* New York: Houghton Mifflin.

[VTP01] Caltech/MIT Voting Technology Project. 2001. *What is/what could be.* Boston/Pasadena: VTP.

[CF02] Carter, J., and G. Ford. 2002. *To assure pride and confidence in the electoral process.* Washington, DC: Brookings Institution Press.

[CSED08] Center for the Study of Elections and Democracy. 2008. *Evaluating the quality of the voting experience.* Provo, Utah: Brigham Young University.

[CMM08] Claassen, R. L., D. B. Magleby, J. Q. Monson, and K. D. Patterson, K. D. 2008. At your service: voter evaluations of poll worker performance. *American Politics Research* 36: 612–634.

[Fo06] Fortier, J. C. 2006. *Absentee and early voting. Trends, promises, and perils.* Washington, DC: AEI Press.

[GH09] Gronke, P., and J. Hicks. 2009. Re-examining voter confidence as a metric for election performance. Paper presented at the annual meeting of the *Midwest Political Science Association,* Chicago, IL: April 2-5, 2009

[Ha09] Hall, T. E. 2009. Voter attitudes toward poll workers in the 2008 election. Paper presented at the annual meeting of the *Midwest Political Science Association,* Chicago, IL: April 2-5, 2009.

[HMP09] Hall, T. E., J. Q. Monson, and K. Patterson, K. 2008. Poll workers and American democracy. In *Democracy in the States: Experiments in Election Reform,* ed. B. Cain, T. Donovan, and C. Tolbert. Washington, DC: Brookings Institution Press, 35-54.

[HMP09] Hall, T. E., Q. Monson, and K. Patterson, K. 2009. The human dimension of elections. How poll workers shape public confidence in elections. *Political Research Quarterly*. 62, No. 3, 507-522

[HNH08] Herrnson, P. S., R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. C. Conrad, and M. W. Traugott. 2008. *Voting technology. The not-so-simple act of casting a ballot.* Washington, D.C.: Brookings Institution Press.

[JP09] Jacobs, B., and W. Pieters. 2009. Electronic voting in the Netherlands. From early adoption to early abolishment. In *Foundations of security analysis and design V: FOSAD 2007/2008/2009 tutorial lectures, lecture notes in computer science, vol. 5705,* ed. A. Aldini, G. Barthe, and R. Gorrieri. Berlin: Springer-Verlag. 121-144.

[KSR04] Kohno, T., A. Stubblefield, A. D., Rubin, and D. S. Wallach. 2004. Analysis of an electronic voting system. In *IEEE symposium on security and privacy.* IEEE Computer Society Press. 1-23.

[Lo08] Loeber, L. 2008. E-voting in the Netherlands; from general acceptance to general doubt in two years. In *Electronic voting 2008, GI lecture notes in informatics,* ed. R. Krimmer and R. Grimm, 21–30. Bonn, Germany: Gesellschaft für Informatik.

[MT04] McNeal, R., and C. Tolbert. 2004. Support for Internet voting in the United States. In *Electronic voting and democracy. A comparative analysis,* ed. N. Kersting and H. Baldersheim. London: Palgrave.

[St09] Stewart III, C. 2009. Election technology and the voting experience in 2008. Paper presented at the annual meeting of the *Midwest Political Science Association,* Chicago, IL: April 2-5, 2009.

[St06] Stewart III, C. 2006. Residual vote in the 2004 election. *Election Law Journal* 5 (2): 158–169.

[TV03] Tomz, M., and R. P. Van Houweling. 2003. How does voting equipment affect the racial gap in voided ballots? *American Journal of Political Science*, 47, 1: 347-361.

[TM05] Trechsel, A. H., and F. Mendez. 2005. *The European Union and e-voting. Addressing the European Parliament's Internet voting challenge.* London: Routledge.

[TSB07] Trechsel, A. H., G. Schwerdt, F. Breuer, R. M. Alvarez, and T. E. Hall. 2007. *Report for the Council of Europe, Internet voting in the March 2007 parliamentary elections in Estonia.* Strasbourg: Council of Europe.

Double-entry Accounting Provides Software-Independent Algorithm for Confirming the Integrity of Automated Election Tallies

Roberto S. Verzola

Institute of Mathematics
University of the Philippines
Diliman Campus, Quezon City
Philippines
rverzola@gn.apc.org

Abstract: This paper proposes the use of double-entry accounting to maintain the integrity of election data as they go through the processes of counting, canvassing, consolidation, and reporting. Double-entry accounting brings to election tallies its well-known benefits of minimizing errors, deterring fraud, and maintaining the integrity of large collections of numeric data. Its superiority to single-entry methods, which are currently in use in the electoral tallies of most countries, is universally acknowledged in business and is increasingly appreciated by governments. This paper describes how double-entry accounting can be applied to election tallies, proposes the equations that govern the accounting of ballots and votes, and discusses the advantages that this brings. It also responds to arguments that the method is not appropriate for election tallies.

1 Introduction

Persistent concerns about the integrity of electronic voting (e-voting) systems have slowed down their adoption in many countries.

One response to this concern is the suggestion to make e-voting systems "software-independent." For instance, the U.S. National Institute of Standards and Technology (NIST), with the support of the U.S. Association of Computing Machinery (ACM), had recommended to the Technical Guidelines Development Committee (TGDC) that only software-independent e-voting systems be certified. The TGDC adopted this recommendation and, in turn, proposed it to the U.S. Election Assistance Commission.

Thus the TGDC Voluntary Voting Systems Guidelines (VVSG) now include software independence as a voting system requirement: "Software independence (Rivest06) means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. All voting systems must be software independent in order to conform to the VVSG" [TG07].

One way to make an e-voting system software independent is to retain a paper ballot as the original document expressing voter intent. Since errors due to software cannot alter the paper ballot, these errors can be detected in a ballot-based recount. Thus in their paper cited in the VVSG, Rivest and Wack call the paper ballot approach "strongly software-independent" [RW06].

This paper proposes the use of the double-entry accounting method to provide a simple, robust, and time-tested way to detect errors in voting machine counts that is also software-independent.

2 Data items as equalities

Double-entry accounting is based on an algorithm that detects errors in real-time from a numeric data set, regardless of its size, by imposing a consistency check on every data item that goes in and comes out of the data set. This consistency check is implemented by requiring every data item to be recorded *as an equality*. As data items are accumulated, recorded, totaled, reported, and rerecorded at various levels of data consolidation, equal amounts are being manipulated all the time. Thus the totals of the left and right hand sides of the equality (henceforth, LHS and RHS) must remain equal *at all times*.[1] Most errors in recording, arithmetic, and reporting will cause the equality to fail. So if the consistency check is done in real-time, errors will be automatically detected in real-time too. This method can detect errors in the original data set–as submitted by optical ballot scanners or human counters, for instance–as well as errors in the data set introduced by the machines, software, or human operators that update, manipulate, and report this data set. As long as the raw data sets are made available, this method can be implemented independently of the specific software or hardware platform used in an e-voting system. The accounting profession implements this automatic checking by recording the two sides of the equality in two corresponding columns, and regularly ensuring that the two columns are "balanced," i.e., their totals are equal.

Over the centuries, businesses and the accounting profession have developed and standardized systems and procedures–familiar to managers, auditors, accountants, and bookkeepers worldwide–for maintaining a generally high level of data integrity using this method, which can be implemented manually or in software. When businesses shift from manual to computerized data operations, more sophisticated means of ensuring data integrity become possible. Still, this highly-robust, time-tested, and standardized double-entry method is invariably retained as a way to keep data operations machine- and software-independent. So it remains a universal workhorse of businesses.

First described in the late fifteenth century, the superiority of the double-entry system to single-entry methods has made it the standard system of business accounting for several hundred years throughout the world.

[1] Accountants call the left-hand side (LHS) of the equality debit (Dr), and the right-hand side of the equality credit (Cr).

Increasingly, double-entry accounting has made inroads in governments too, although they have been slower in recognizing its benefits. It was only in the nineteenth century when it saw widespread use in the public sectors of France (1815) and Great Britain (1829) [Ni01]. Some countries adopted the system only in the late twentieth century. In the first few years of the twenty-first century, the European Commission was still using single-entry accounting [Kh02], shifting to the double-entry system only on 1 January 2005 [EU06]. In other countries, especially among local governments, its introduction is still in the planning stages, as part of public sector financial reform.

It is therefore understandable if election authorities have not yet made the conceptual leap to adopt double-entry accounting in vote tabulations.

3 Election tallies today: single-entry

Most election tallies today still use the single-entry accounting method of recording and accumulating individual isolated numbers, not equalities. This method is susceptible to undetected errors that can be passed on to intermediate levels of vote consolidation up to the final tabulation. The common practice of recording, maintaining, and reporting vote totals at every level of consolidation is *not* double-entry accounting. Few election authorities strictly enforce a requirement that blanks (or undervotes) and invalid votes (such as overvotes) be counted, recorded, reported, and included in the totals at every consolidation level, in the same way that votes for candidates are. If small unexplained discrepancies arise which are deemed immaterial to the final outcome, local voting officials tend to simply agree to "clean up" the figures. Few, if any, set aside special accounts to keep track of small discrepancies that could not be reconciled in time. Since special accounts such as blanks, invalids, missing, and excess votes are necessary to implement a true double-entry election accounting system, there cannot be many countries, municipalities or election jurisdictions, if indeed there is even one, that use this system in vote tabulations and election accounting today.

4 Every vote counts

It is sometimes argued that the requirements are more stringent in accounting for money than in accounting for votes. According to this argument, a win by a small margin is no different from a win by a large margin. Hence, the argument goes, accuracy to the last vote is not as important as accuracy to the last cent.

On the contrary, accuracy to the last vote is also important for the following reasons:

- A single vote may not make a difference to an election outcome, just as a single cent hardly makes a difference to a businessman's bottom line. But a one-vote or one-cent discrepancy may hide larger, but undetected discrepancies in the system. Worse, they may indicate procedural or system flaws or loopholes that can result in more serious errors in the future. Businesses take one-cent discrepancies seriously not because one

cent matters to them, but to make sure that the discrepancy does not hide more serious problems in their accounting system. Just as banking automation made possible large-scale fraud through the accumulation of fractional cents and round-off errors, election automation makes possible fraudulent election outcomes through the accumulation of small discrepancies in many voting precincts. Through its simple consistency check of equalities, the double-entry algorithm can detect even single-vote discrepancies, as soon as they occur. This imposes, at very low cost, a high-quality standard for election data sets and voting machines, which can only enhance the public perception of e-voting systems.

- The size of a winning margin is significant as far as a winner's mandate is concerned. Thus, vote discrepancies may not affect the final outcome, but they may still affect the publicly-perceived mandate or lack of mandate of an election winner. In the 2004 Philippine election for president, for instance, the winner who was eventually proclaimed was secretly caught in taped telephone conversations, subsequently made public, as she instructed a senior election official in manipulating election results to ensure herself a winning margin of at least one million votes.

- In many countries, the sanctity of the ballot is enshrined in their constitution, which emphasizes that every single vote–and voter–counts. To win public trust, it is best that e-voting system vendors adopt a similar attitude.

5 Basic features of a double-entry election tabulation system

This paper describes the basic features of a double-entry election tabulation system for a one-slot position (e.g., president) and for a multiple slot position (e.g., senator, where twelve slots are available in the Philippine case). The examples given are also applicable to other single- or multi-slot positions. It is assumed that voter-prepared paper ballots are used, for scanning by optical ballot scanners.
In business accounting, the fundamental equalities are **Assets = Capital + Liabilities** and **Revenue = Expenses + Profit**. In double-entry election accounting, the fundamental equalities are discussed below.
Ballots are the heart of the election process, because they represent a permanent record of voter intent, the "will of the people." In keeping track of ballots, the following **ballot equation** can be used:

Received Ballots + Excess Ballots = Cast Ballots + Spoiled Ballots + Unused Ballots + Missing Ballots

Received Ballots record the number of ballots allotted to the voting jurisdiction. Ballots end up as either **Cast** (i.e., given to the voter and filled out), **Unused**, or **Spoiled**. The total ballots cast, unused or spoiled should equal the number received, which accounts for every single ballot, at every level of consolidation. The **Excess** and **Missing** accounts are used to force a balance and transparently record anomalous situations where some ballots could not be accounted for, even after repeated efforts to do so.

6 The ballot status report

Table 1 shows a sample ballot status report for one precinct, based on the ballot equation:

Table 1. Ballot Status Report		
Ballot type	LHS (Dr)	RHS (Cr)
Received	200	
Excess	0	
Cast		45
Spoiled		3
Unused		152
Missing		0
Column Total	200	200

Under Ballot Type, the RHS accounts (Cast, Spoiled, Unused, and Missing) are indented, in accordance with common accounting practice. The LHS of the two numeric columns represents the total number of ballots received by the polling center. The RHS breaks down how these ballots ended up. The LHS total is equal to the RHS total and the report is balanced. If an imbalance exists, the reason for the discrepancy must be identified and corrected. If it persists–which is anomalous–and time does not permit another round of double-checking, the discrepancy should be recorded on the side that is smaller, as Excess or as Missing. This balances the report in a transparent manner, which allows for a subsequent audit later if the Excess/Missing accounts appear abnormally high.

In every ballot are the votes, the key to the whole process. Two equations govern the accounting of votes:

No. of Slots for Position x Cast Ballots = Available Votes
Available Votes + Excess Votes = Valid Votes + Invalid/Blank Votes + Missing Votes

For executive positions like president or vice-president, there is only one slot for the winner. Hence, the number of validly cast ballots is also the number of total available votes. For legislative positions like senator or councilor, there are usually several slots, fixed by law. Then, the number of total **Available Votes** is the number of validly **Cast** ballots multiplied by the **number of slots** available for the position being contested. Available votes can end up three ways. They can be cast as **Valid** and counted in favor of a particular candidate. They can be deemed **Invalid**; for example, a non-candidate is voted in or if two names or more are listed or marked (also called an “overvote”), or for any other reason as defined by law. Finally, an available vote can remain **Blank** (also called an “undervote”). The total votes counted in favor of each candidate plus the

Invalid/Blank votes should equal the Available Votes. The Caltech/MIT Voting Technology Project lumps together all Invalid/Blank votes that did not go to any candidate under the term "residual" votes, and studied the role of variations in county, technology, demography, and other factors that tend to increase or decrease them [AS04].

The vote equation was separately proposed in 2004 by Saltman as well as by Jones. Saltman suggested that "for each contest, the total number of ballots cast multiplied by the number of legitimate votes cast per ballot should equal the sum of votes assigned to each candidate plus the number of overvotes plus the number of undervotes". [Sa04]. Jones proposed essentially the same equation B = C + O + U, where B is the number of "ballots found in the ballot box," C is the "sum of votes for specific candidates," O is the "number of overvotes," and U the "number of undervotes" [Jo04]. Writing about e-voting systems, both authors also referred to double-entry methods, but in the context of financial transactions and business accounting. Saltman wrote: "As in accounting, where double-entry bookkeeping has been standard for about a century, there needs to be cross-checking that distributes the total responses possible with each ballot to each category that could have been used by each user" [Sa04]. And Jones wrote: "Thus, we issue carbon copies of the paper receipt for a financial transaction to both parties in the transaction, and we develop systems such as double-entry bookkeeping" [Jo04]. Neither author, however, proposed setting up special Excess or Missing Accounts, which are essential to an auditable double-entry accounting system in election tallies.

7 Vote status report: single-slot positions

Table 2. Vote Report, for President		
No. of Slots: 1	Cast Ballots: 150	
Votes	LHS (Dr)	RHS (Cr)
Available	150	
Excess	0	
Invalid/blank		12
Candidate 1		70
Candidate 2		50
Candidate 3		18
Missing		0
Column Total	150	150

Table 2 is a sample vote report for a single-slot position in one precinct, where candidates 1, 2 and 3 are hypothetical candidates.

Available Votes is equal to the No. of Slots times the Cast Ballots in the Ballot Report (taken from Table 1). Invalid/Blank Votes are the slots which have been left blank, which contain unrecognizable names, or which were not counted for one reason or another.

Procedure-wise, the main difference between the double-entry and single-entry methods is the extra work, throughout the consolidation process at every level, of keeping track of invalid/blank votes–votes in a validly cast ballot that did not go to any candidate. This extra work is equivalent to an additional candidate in every position. *This data is essential in a double-entry election accounting system, to make possible a balanced vote report.*

As in standard accounting practice, the LHS and RHS column totals (debits and credits in accounting parlance) must balance before the next step in the process can proceed. The Excess/Missing accounts can be used to force a balance in a transparent way, to document unexplained discrepancies in the count. These should also be recorded, added up, and reported throughout the process, at every level of consolidation.

8 Vote status report: multiple-slot positions

In multi-slot positions, voters may write several names on the ballot for the same position. In this case, Available Votes is equal to Cast Ballots (this number is taken from the Ballot Status Report, Table 1) times the No. of Slots (1,800 equals 150 times 12). Table 3 below is a sample vote report for a multi-slot position in one precinct.

Counting the invalid/blank votes in a multi-slot contest is only slightly more complicated, because each ballot may hold a mix of valid and invalid/blank votes. Aside from the valid votes per candidate in the contest, the number of invalid/blank votes in the ballot must also be counted and recorded. Note that for each position, the total of the valid votes per candidate plus the Invalid/Blank Votes should always equal the number of slots available for the position (12, in the example given).

Table 3. Vote Report, for Senator		
No. of Slots: 1	Ballots cast: 150	
Votes	LHS (Dr)	RHS (Cr)
Available	1800	
Excess	0	
Invalid/blank		640
Candidate 1		110
Candidate 2		105
Candidate 3		100
Candidate 4		95
Candidate 5		90
Candidate 6		85
Candidate 7		80
Candidate 8		75
Candidate 9		70
Candidate 10		65
Candidate 11		60
Candidate 12		55
Candidate 13		50
Candidate 14		45
Candidate 15		40
Candidate 16		35
Missing		0
Column Total	1800	1800

9 Special accounts: the Excess/Missing accounts

Election officials point out that a vote count at the precinct level often ends up with a few extra or missing ballots or votes which could not be accounted for. Then they simply agree among themselves to sweep these small discrepancies under the rug and send in a report with consistent totals.

Under a true double-entry system, separate accounts (often called "errors and omissions") are created and maintained, so that discrepancies which cannot be explained within the time available to the election authorities are transparently recorded under such accounts, thus maintaining the required balance between the two columns. These accounts can be called Excess (a LHS account) and Missing (a RHS account). The following algorithm will force a vote report to balance:

- compute the difference between the two column totals;
- record the difference under the column with the smaller total, as Excess if the LHS-column total is smaller or as Missing if the RHS-column total is smaller;
- recompute the column totals, which should now balance.

The Excess/Missing accounts record a potential vote padding/shaving problem, which election officials are unable to resolve immediately. Documenting the forced balance in such a transparent manner facilitates a subsequent audit should it prove to be necessary.

These accounts should be maintained, recorded and reported at every level of consolidation, together with vote and ballot counts.

10 Advantages of double-entry election accounting

If governments are slow to recognize the superiority of double-entry election accounting, the private sector, including the e-voting industry, can take the initiative in its advocacy, citing their current business accounting practices. The latter, for one, should welcome the strict consistency check on the data, which facilitates machine and software testing, helps improve software quality, and gives them more confidence in the internal consistency of their system, a clear marketing advantage. For governments, election authorities and the ordinary voter, double-entry election accounting will bring the following specific advantages:

- The double-entry method is a simple, easy-to-understand, highly standardized, and widely-known algorithm for enforcing data consistency that has withstood the test of time. Its universal use in the business sector and widespread use in the government sector attests to its superiority over the single-entry election tabulation method that is used today in most countries and localities. Failure to balance is an automatic warning about problems in the election data set. It can flag clerical errors such as recording or addition mistakes that often creep in and stay undetected when single-entry methods are used, or errors introduced into the data set by the machine or its software. It can also locate errors more easily by testing which section of the data set fails to balance.

- It provides a logical step-by-step upgrade path for electoral reform and modernization. In countries like the Philippines, where the manual system of election tabulation itself suffers from substantial flaws [Ca04], undertaking automation before existing systemic flaws themselves are corrected seems foolhardy. Introducing a new level of complexity on a shaky foundation of uncorrected systemic and procedural defects is a formula for expensive failure. Automating a flawed single-entry system could result in an equally flawed automated system that would sooner or later have to be redone. Given the costs and risks associated with any automation project, it would make sense for countries which are considering election automation to first modernize their tabulation system by adopting double-entry accounting. This simple, low-cost step can tap existing pools of expertise that even the least developed countries already have and immediately provide dramatic improvements in minimizing clerical errors, maintaining the integrity of election data, and deterring fraud.

- On the stable platform of a modern election accounting system, countries may choose to upgrade to an intermediate hybrid system that uses spreadsheet software to implement the modernized method with computers, or they can skip this step and proceed directly to full automation, using the same double-entry system. In each upgrade step towards automation, the double-entry system provides a built-in check during the period of conversion that facilitates the process, in a way that is independent of vendors, machines, and software. Existing voting machines outputs in standard formats like Comma Separated Values (CSV) or Election Markup Language (EML) can be fed to third-party software to check for consistency using the double-entry system. Later, vendors may add an accounting module in their software to tally votes using double-entry methods, as an option or as a standard feature. Whether the election only covers one position (typical in the European context) or many (as in the U.S. and Philippine context), implementing the double-entry method involves the equivalent of accounting for the votes of an additional candidate. At worst, this means 50% more work if there are only two candidates vying for a position. In jurisdictions that are required to keep track of invalid/blank votes anyway, then this is not additional work at all.

- Strictly enforcing the requirement that reports balance will instill among election officials the discipline of providing necessary information which may not relate directly to the question of who won or lost the elections, but which is essential in detecting errors and other anomalies. This information includes the number of invalid/blank votes, the number of ballots cast (or voters who actually voted), the number of excess/missing ballots, and the number of precincts tallied. Under single-entry methods, the discipline of submitting such information may be imposed through instructions and administrative orders, but local election officials may simply ignore the requirement. In the Philippines, for instance, one-third (thirty-three out of ninety-eight) of the cities and provinces submitting their reports to the National Canvassing Board in the May 2007 elections did not provide the number of precincts tallied or the number of voters who actually voted [Ha97]. Under double-entry accounting rules, officials have no option, but to provide this information or the reports will not balance. Election officials may still force a balance by using special accounts specifically meant for this purpose, but doing so will make such moves transparent and subject to subsequent audit.

- The data consistency imposed by the double-entry system sets high-quality standards among e-voting vendors, forcing them to seriously check every single vote discrepancy in their machines and their software. In so doing, it enhances the public perception of the integrity of e-voting systems. While voting machines today do incorporate their own internal data checks, these checks may vary from one vendor to another, from one software to another, and from one model to another. A change of vendor, model or software version can introduce new problems that may not be detected in time, allowing errors to creep to higher levels of vote consolidation. By adopting an election tabulation platform that is independent of vendor, machine or software, mistakes and errors can be detected as soon as they are made.

- The additional information requirement to implement double-entry election accounting facilitates fraud control. The number of invalid/blank votes and the number of ballots cast set an upper-bound on the fraudulent votes that a dishonest candidate may accumulate and help detect ballot stuffing or its electronic equivalent. The number of excess/missing ballots, if significant, can trigger deeper investigation. The number of precincts tallied enables the computation of per-precinct averages and other statistics, which are useful indicators for detecting abnormal events, such as highly improbable or even impossible statistics as well as wild swings in some averages.

11 Limitations

Double-entry accounting should not be seen as a magic bullet that will eliminate election fraud. Even in business, where double-entry methods have been in use for several hundred years, fraudulent business practices continue to be uncovered and business owners as well as consumers must remain vigilant. For instance, double-entry methods will have no effect on electioneering with government resources, election overspending, or vote-buying. It cannot prevent the suppression of votes caused by fouling up voters' lists, precinct assignments or precinct locations. It cannot prevent goons from taking over voting precincts and operating the voting or counting machines directly. For best effect, it needs to be used together with other tools for fraud detection, investigation, and control.

In particular, two common errors will not be detected. If two erroneous, but offsetting errors are recorded, preserving the equality in the two columns, the errors are not detected. Thus, the double-entry method will not detect a vote padding/shaving operation where votes are subtracted from one candidate and the same number of votes is added to another candidate. If two entries in one column are switched, the column total will also stay the same. Thus vote switching between two candidates will not be detected either.

Despite its limitations, double-entry accounting will catch most clerical errors and a number of intentional errors, as every business will testify. It will make it more difficult for fraudulent entries to enter the system, and will save time that would otherwise be spent in detecting, locating, and correcting the errors that managed to creep in. Thus the double-entry approach is still recognized as an enormous advance compared to single-entry systems in minimizing errors, improving auditability, and reducing fraud.

12 Conclusion

Ballot and vote tabulation can benefit significantly from standard double-entry business accounting methods, which involve the recording of equal values at all times. By replacing the single-entry election tally methods practiced today in most countries with double-entry methods, slow election counts due to endless disputes over errors can be avoided and canvassing fraud can be detected more easily.

Bibliography

[AS04] Ansolabehere. S., and C. Stewart. 2004. Voting technology and uncounted votes in the United States. *Journal of Politics*.

[Ca04] Carlos, C. et.al. 2004. *Electoral reform in the Philippines. Issues and challenges,* 89-92.

[EU06] EU Committee of the UK House of Lords. 2006. *Financial management and fraud in the European Union. Perceptions, facts and proposals (Vol. II: Evidence)*.,61. http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/270/270ii.pdf/.

[Jo04] Jones, D. 2004. Auditing elections. *Communications of the ACM, 47* 10: 46-50. http://portal.acm.org/citation.cfm?id=0922594.1022622/.

[Kh02] Bashir K. 2002. The European Union fails on financial accountability. *Contemporary Review*.

[Ha07] Halalang Marangal. 2007. *A citizens' Audit of the 2007 senatorial elections. Report #4.* July 19: 3.

[Ni01] Nikitin, M. 2001. The birth of a modern public sector accounting system in France and Britain and in the influence of Count Mollien. *Accounting History* May.

[RW06] Rivest, R.; Wack, J. 2006. *On the notion of "software independence" in voting systems (draft version)*. July 28, 2006.

[Sa04] Saltman, R. 2004. *Requirements for the evaluation of voting system security*. (presented to the Technical Guidelines Development Committee of the Election Assistance Commission of the U.S. National Institutes of Standards and Technology). Sep. 20. http://vote.nist.gov/NISTpaper%20040920.pdf/.

[TG07] Technical Guidelines Development Committee. 2007. *Voluntary voting system guidelines recommendations to the election assistance commission.*

Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria

Andreas Ehringfeld[1], Larissa Naber[1], Thomas Grechenig[1],
Robert Krimmer[2], Markus Traxl[3], Gerald Fischer[1]

[1]Vienna University of Technology
Industrial Software (INSO)
1040 Vienna, Austria
{firstname.lastname}@inso.tuwien.ac.at

[2]E-Voting.CC gGmbH
Competence Center for Electronic Voting and Participation
1190 Vienna, Austria
r.krimmer@e-voting.cc

[3]Institut für Verwaltungsmanagement
6020 Innsbruck, Austria
markus.traxl@verwaltungsmanagment.at

Abstract: This paper discusses the recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting in light of the various attacks against the 2009 Austrian federation of students election. This election was the first instance of e-voting being implemented in a legally binding election in Austria. The question is if the recommendation published in 2004 is sufficient to handle real-world attacks against elections using e-voting. Based on the experience gained, several amendments to the recommendation are described.

1 Introduction

According to [BSSL01] and [SZKK88] regular re-evaluation and re-assessment are fundamental security principles. The recommendation Rec(2004)11 on legal, operational and technical standards for e-voting [Rec04] of the Committee of Ministers to member states was developed by [CEIP04] between 2002 and 2004 and remained unchanged so far.

The effectiveness of Rec(2004)11 is analyzed based on the experience of a recent e-voting election, which suffered from various different attacks such as the first Denial of Service attack (DoS) against a legally binding electronic election worldwide.

1.1 Case Study: 2009 Austrian Federation of Students Elections

The Austrian federation of students elections (*Hochschülerinnen- und Hochschülerschaftswahlen*) takes place every two years. Of the 240,000 eligible voters only about 30% participate in the voting (average for the past thirty-six years). The voting period is three days long during which students at all universities in Austria can cast their votes. Prior to the 2009 election, paper-based voting was the only channel.

The idea using electronic voting for the federation of students election was first introduced in May 2000 by the national federation of students. As a consequence of [OeH00], the federation of students law was adapted to allow for the possibility of remote voting like e-voting or postal voting. This amendment led to an evaluation project [EV07] with the heads of the national federation of students and members of the Austrian ministry for science, focusing on e-voting at the University of Economics in Vienna.

In May 2007, the minister for science and research announced that e-voting would be an additional voting channel in the 2009 federation of students election. The project's goal was to enable students (such as students currently abroad) to cast their votes from home.

Four months later, the national federation of students published a statement in [OeH07] summarizing their objections to e-voting and concluding that the technology conflicts with the idea of a free and secret ballot. Despite the fact that the threats concerning e-voting are similar to those in almost all other modes of voting, especially all modes of remote voting (e.g., [AH04] and [AH08]), e-voting (and the risks involved) became a very controversial topic and thus one of the major topics of most election campaigns [OHER10].

Other than federation of students' resistance, the federation of students election made for a very good field study because it has a very high organizational complexity, despite the small number of potential voters (260,000), with more than 400 individual voting options across the twenty-one participating universities. The required technical skill and in-depth knowledge of the election process can rival any other Austrian election.

1.2 Methodology

The Edwards Deming Plan-Do-Check-Act Cycle (PDCA Cycle) [ED50] can be employed to improve upon Rec(2004)11.

Plan (Hypothesis): The question is whether the recommendations in Rec(2004)11 are sufficient to handle state-of-the-art real world attacks.

Do (Experiment): The 2009 Austrian federation of students election was chosen for this analysis because it is a recent example of a legally binding e-voting election, which used the Rec(2004)11 as a benchmark in the certification process and caused much controversy, which guarantees a high number of skilled attacks. The voter base - students - are skilled, creative, personally motivated, and equipped with both technical resources and enough time to plan and execute attacks. This makes them a force to reckon with.

Check (Evaluation): The various attacks during the electronic voting period are described; countermeasures are explained and related to the recommendations in Rec(2004)11. Identified gaps are analyzed and conclusions drawn. Potential amendments for further improvement of Rec(2004)11 are presented.

Act: The final step in the Deming Cycle lies within the biennial review cycle of Rec(2004)11 where additional recommendations and updates are discussed in detail.

1.3 Related Work

Related work deals with security relevant aspects of e-voting from different views. The legal bearings of e-voting at the Austrian federation of students election are discussed in [KLSV09; LC10]. Papers like [SLBV09] show technical requirements while [XAMA05] deals with the procedural security and social acceptance in e-voting.

2 Recommendation Rec(2004)11 for E-Voting

As part of the project [CoED04] the Committee of Ministers established an expert committee to prepare recommendations on legal, operational, and technical standards for e-voting in the years 2002–2004. The standards were adopted as Rec(2004)11 on 30 September 2004.

The measures included in the Recommendation are grouped into legal standards (thirty-five measures), operational standards (twenty-five measures), and technical requirements (fifty-three measures).

A continuous improvement process over a biennial cycle forms an integral part of the Recommendation. Currently additional recommendations derived from the experiences gained in recent projects are in discussion (see [CoEO10]). These amendments pertain to election observation and the certification processes of e-voting systems.

3 Certification of the E-Voting System of the 2009 Federation of Students Election Based on the Recommendation Rec(2004)11

The timeline, activities, and responsibilities of the federation of students election are defined in the federation of students law [HSG98] and the election regulations [HSWO05]. Concerning e-voting this means that although the specifications are technology neutral and non-discriminatory, they shape how e-voting is implemented. The legal framework stipulates - among other aspects - that the e-voting system has to be approved by the Austrian data protection commission. Furthermore a certification process based on Common Criteria and the recommendation Rec(2004)11 has to be passed.

The technical components to be used—especially those related to the vote casting and the voters' authentication—have to be certified sixty days before the election by a certification authority according to the laws [Sig10], [HSG98] and election regulation [HSWO05].

The e-voting software (documentation, development process descriptions, architecture, security descriptions, threat analysis, technical descriptions, and source code) was audited between December 2008 and March 2009. On 27 March, the certification process ended successfully with the publishing of a certification [ASC09]. The published certificate stipulated key types and length, the compliance of processes for compilation, installation, configuration and operation of the software as well as operating conditions and security information to be released to the voters.

4 Technical Attacks during the E-Voting Period

E-voting, as a new voting channel in the 2009 Austrian federation of students election, was scheduled to be completed before the traditional on-site paper-based vote. Thus voters were able to cast their vote electronically between 18 May at 8:00 AM and 22 May at 6:00 PM. Students could choose whether they wanted to cast their votes electronically or vote in the traditional paper-based election between 26–28 May.

During the e-voting period, different attacks against the e-voting system, voters' acceptance, and the elections were discovered. Several of those attacks are described in the following sections.

4.1 Distributed Denial of Service Attack

Three days before the electronic election started preparations of a distributed Denial of Service (dDoS) attack were detected by the e-voting provider's security staff. An Austrian organization, registered as an organization working toward the use of information technology and telecommunication in a humane, socially responsible and private way, published a web tool which was touted as a harmless server availability checking tool. It was stated that everyone has the right to stress test (check the availability of) the e-voting system, and therefore it was absolutely legal, and practically mandatory, for as many people on as many PCs as possible, to do so, preferably day and night.

Fig. 1: GUI of the dDoS attack tool

The tool was written in javascript and opened a certain URL in invisible iframes as specified within a form textbox on the webpage (per default prefilled with the e-voting website). To avoid browser caching, random characters were added at the end of the URLs opened by the iframes. The other parameters defined how many iframes were opened/refreshed at the same time and at which interval. As the Austrian Computer Emergency Response Team (CERT.at) analyzed the potential danger of the script, even a brief analysis showed that a single PC using commonplace ADSL connectivity produced a permanent load of 10 Mbit/s on the web server.

The most interesting aspect of this attack is that although it was managed centrally, the attackers were distributed using their local resources and their local IP, which made the detection of attackers and possible blocking harder. Unlike most dDoS, this attack did not require a bot-net to be in place; the attackers participated willingly, even if sometimes unwittingly, to the potential problems caused.

An effective technical countermeasure to stop the attack was to include code written in javascript on every webpage of the e-voting system, which checked if the site was opened within a frame and reopened the site within the parent window, thus effectively stopping the tool.

This attack highlighted several of the practical problems stemming from denial of service attacks on e-voting systems. Even though dDoS attacks are not limited to e-voting systems, the ramifications of dealing with them in an e-voting setup are different. Blocking all incoming traffic from the source IP is a common measure. In an e-voting situation, this might deprive an unknown number of other voters of their legal voting rights. Configuration changes and parameter, or even software, adaptations are other popular counter measures. Again in the case of an e-voting system, it has to be considered whether these measures invalidate the existing certification and thus disqualify the whole election. The problem might be compounded by several adaptations

on the attackers' side forcing even more adaptations on the e-voting systems. These questions mostly belong in the realm of law and likely will keep legal practitioners occupied for years.

In case of the Austrian federation of students election, configuration changes were not necessary as the javascript code was already part of the e-voting system and certified months before. The original intention of the existing codes was to keep political parties and others from directly including the voting system via frames as part of their webpages. The same code was added to the gateway pages to also protect those pages from being attacked. As these pages were not part of the certified voting system, no conflicts resulted.

The most important countermeasure however was that e-voting was an additional voting channel scheduled before the paper-based election. According to the law, the election commission can—in the case of specific problems—decide to annul the e-vote, and the students who already voted electronically would be advised to vote again during the paper-based voting period. Consequently not even a successful dDoS attack can effectively harm the election. We suggest to amend the existing paragraph within Rec(2004)11 (art. 45) to not only state that "*remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations…*" but also to include a statement that ending the remote election period before the opening of the polling stations and establishing a process for informing all remote voters in case of annulment due to technical problems may be a way to countermeasure the effect of a dDoS attack.

4.2 Phishing Attack with Mock E-Voting System

To successfully cast a vote students using their own personal computer had to use an Austrian citizen card [BK10], a card reader, and an internet browser with java support. To access the voting system the students had to visit the official federation of students election website, http://www.oeh-wahl.gv.at [OeW10], where they received all relevant information concerning the election. The e-voting system was only linked to the official federation of students election website during the actual e-voting period. The link to the voting system was not published in advance. By clicking a link marked "to the electronic voting," the students were transferred to the voting system.

During the voting period, a political party published a website similar to the official website to mislead the voters. Even a voting process was simulated. The URL used was easily mistaken for the official URL:

Official URL:	www.oeh-wahl.gv.at
Attacker's URL:	www.oeh-wahlen.at
Differences:	election vs. elections (translated) and missing government (gv) subdomain.

This attack could be considered as a phishing attack to gain sensitive information or, at the least, to irritate and mislead the voters. Phishing attacks are not e-voting specific so there are many anti-phishing approaches like [MP08] in banking or [QRYM07] in e-mail systems.

From the technical point of view, this attack could be counteracted by a combination of several measures. First of all, an official website of the election has to be established. It should be the single point of official information concerning everything related to the election. This especially includes the time the election takes place, the description of the voting process, the locations of the polling stations, the names of the candidates and political parties, results of previous elections, and the final results of this election. Furthermore this official website should be the portal to the e-voting system during the e-voting period. The website should be announced through multiple channels such as posters, links from other trustful websites, and much more which reflects Rec(2004)11 Art. 46 which states, "*For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.*"

Evaluation of the referrer HTTP header in the portal server logs showed that about 42 percent of the visitors directly navigated the website by entering the official URL manually into the browser. Most other visitors searched for the name of the election using their favorite search engine (keywords: "federation of students election, information, e-voting" before the election, "federation of students election, e-voting" during the election period, "federation of students election, results" after the election). Consequently active monitoring of search engine results on typical queries and decisive action against phishers are essential countermeasures against such phishing attacks. Buying domains easily mistaken for the real URL and therefore likely targets for phishers is another appropriate countermeasure.

As described in [QSM07], proofing the integrity of the website is very important which concludes to the recommendation to use extended validation certificates (EV) which add verified identity to SSL as described in [CF11]. Furthermore, official websites and internet voting systems related to legally binding elections should be hosted within the government domain space (in Austria e-voting.oeh-wahl.gv.at).

From the organizational point of view, the political party's fake website conflicts with the principles of honest e-voting based on the experience of internet voting in the Estonian parliamentary elections [TSBA07]. In the Austrian federation of students election all election commissions and political parties were made aware of the principles, which were recommended by the Council of Europe, however, never accepted.

Different studies have shown that server-side security indicators and client-side mechanisms like browser warnings do not guarantee prevention of phishing attacks [DHC06] [DTH06] [SDOF07] [WIFE05] [WMG06]. This is due to the fact that if phishers can convincingly imitate the appearance of legitimate web sites, users tend to ignore security warning or do not interpret security cues appropriately [YWAP08]. As an

additional technical countermeasure, the security layer of the Austrian citizen card used for authentication per default only allows access to the personal data stored on the card if the connection is based on HTTPS and the requested data is either sent to a .gv.at domain or a domain identified by a special certificate denoting the URL as a government related resource. Naturally neither .gv.at domains nor a government OID certificate are freely obtainable. For further details on the security architecture of the Austrian citizen card, please refer to [LHP02].

From the operational point of view, before and during the election period the registration and use of domain names similar to the official domain name have to be strictly monitored. Any suspicious activity should be brought to the attention of the election commission as soon as possible to allow for enough time to instigate counter measures.

Even though this advice is not explicitly included within Rec(2004)11, it is addressed by article 103: "*The audit system shall record times, events and actions, including: [...] any attacks on the operation of the e-voting system and its communications infrastructure [...] malfunctions and other threats to the system.*" Nevertheless, considering the danger of such an attack, a paragraph denoting the importance of preventing and handling phishing attacks in remote elections would lead to further improvement.

4.3 Vote Flipping Video

E-voting systems are susceptible to a class of attacks that usually does not feature in other web-based attacks: campaigns to discredit, or smear campaigns. The aim of these attacks is not to disturb or subvert the voting process as such, but to foster the rejection of e-voting as a viable voting channel by alluding that the e-voting process was either not secure or even subverted. Most of the arguments brought against e-voting can be used against any form of remote voting. However, there is one class of arguments that only pertains to e-voting systems and that is the inherent lack of transparency in computerized systems. The technology involved is usually beyond the grasp of the average citizen, and the fact that the same technology powers everything from banking to telecommunications, does not stop people from believing, that this technology will be subverted to nefarious purposes once applied to e-voting.

A vote flipping video was used in a campaign to discredit the federation of students election. This video tried to prove that a voter could select one candidate while on the electronic ballot sheet a different candidate would be marked. The video was released to the media during the election phase.

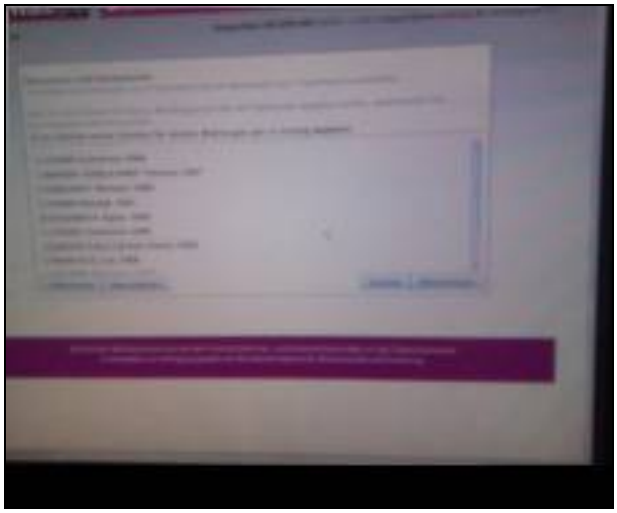


Fig. 2: Fake vote flipping video

Although the video was quite blurry and of bad quality, it was identified as a fake by experts after some investigation. Nevertheless, this experience of the 2009 Austrian federation of students election demonstrates several important aspects. First of all, an incident response team has to be established to react to such events and support the election commission with the analysis as stated in Rec(2004)11 (art. 76): "*Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.*"

Furthermore to allow the timely reaction to attacks, a public communication channel has to be established and announced beforehand. The communication channel should also serve as a contact point for the press in the case of suspicious materials offered to the media. It should be made clear that proof of failure or other reproaches addressed to the media should be handed in for validation before publishing.

Based on this experience it is advisable to declare an official communication channel for announcing possible security relevant incidents. This can be reflected in the appropriate manner in the recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting.

4.4 Vote Buying Campaign

The federation of students election suffered from a second campaign to discredit it, this one a case of alleged vote buying. On the first e-voting day, flyers were found in several lecture rooms at a university asking students to cast their votes using the e-voting system in front of a specific political party's election observers to receive a payment of fifteen euros.

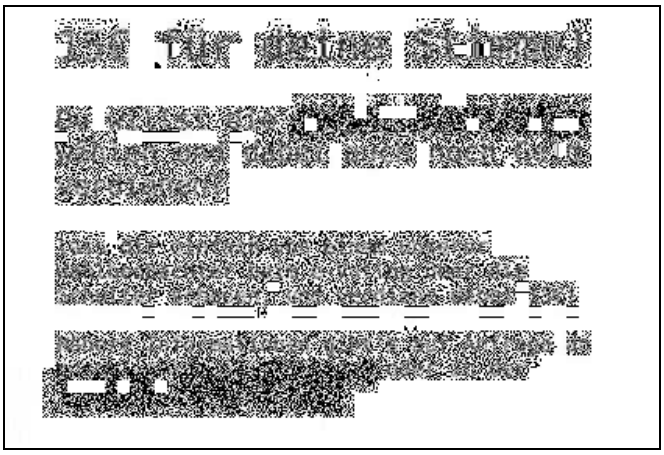


Fig. 3: Flyer for vote buying

Translation:

> 15 € for your vote!
> Do you want to vote for [XXXXXXXX] and at the same time earn money for it?
> Let one of our election observers watch you vote electronically and earn 15€ at the same time.
> Per request, more information is available at [XXXXXXXX]
> or at [XXXXXXXX].

Please note that the names of political parties have been removed.

Although not absolutely proven, it seems relatively certain that the flyers were a fake. The intention of the vote buying flyers could have been not only to discredit the political party named on the flyers, but also to irritate and discourage students eligible to vote from using the e-voting system. However, the e-voting system might not have been the primary target in that case.

Vote buying is the most regular form of violation according to [CAPA07]. If votes are cast in secret, there is no way for candidates and party organizers to be certain that the vote was cast according to the agreement between the voter and the briber. Vote buying is possible for all forms of remote elections and thus not unique to the e-voting process. Rec(2004)11 includes this requirement by several recommendations that have to be

combined to be effective. (art. 80) "*The e-voting system shall restrict access to its services, depending on the user identity. User authentication shall be effective before any action can be carried out."* And (art. 51) *"A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.*" In the 2009 Austrian federation of students election, the voter had to confirm with the digital signature of her/his citizen card that she/he votes free and in secret. This confirmation was an integral part of the authentication process in which the voter's identity was proven by verifying the digital signature. As with any security related system, it is necessary to balance security with usability. The benefit of enforcing such a confirmation at the beginning of the voting process is that the voter's awareness is improved and confirmed before filling out the ballot sheets.

In general Rec(2004)11 should include the recommendation of establishing the voter's awareness that votes should be freely cast and in secret in remote elections.

4.5 Unknown Social Engineering Attacks

During the e-voting period, user-support was handled by the Federal Computing Centre of Austria (BRZ). Voters could contact user-support by e-mail, phone or by an online contact form. A self diagnosis tool, which was integrated within the website, turned out to be very helpful in debugging problems on the user/client side.

As stated in Rec(2004)11 (art. 79), "*The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.*" A technical monitoring system was established to ensure that during the polling period, the voting equipment and its use satisfied the requirements. A traffic light display showed the operations team the functional status of the system without having physical or virtual access to the sealed system. The user-support team was well-trained, especially against social engineering attacks. Processes had been established to identify and counter such malicious attempts.

5 Conclusion

The recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting was published in 2004. Since then there have been periodic iterations by means of biennial review meetings to revisit the impact of the recommendations and to identify necessary amendments.

The focus of this paper was the question of whether the described recommendations are sufficient to handle these state-of-the-art attacks. The basis of this analyze was a discussion of the various attacks that occurred during the 2009 Austrian federation of students election with conclusions regarding suggested improvements for Rec(2004)11.

Based on the distributed denial of service attack, it is a possibility that if e-voting is an additional voting channel, mechanisms could be put in place to recast the vote on election day on paper.

The danger of phishing attacks turned out to be very critical. Therefore Rec(2004)11 could be further improved by explicitly pointing out the necessity of implementing adequate countermeasures.
The acceptance of e-voting as a new voting channel is a key success factor in every project. Various attacks don't target the election directly, but rather target the voters' acceptance by publishing, for example, fake videos of vote flipping as happened during the 2009 Austrian federation of students election. Dealing with such attacks is very difficult and demands the development of a special security strategy, which should be recommended in Rec(2004)11.

Counteracting attack attempts against the e-voting system by social engineering methods demands awareness programs, trained staff, and well-designed processes as requirements that could be included in the recommendation.

The recommendation Rec(2004)11 has been reviewed in 2006, 2008 and will undergo a third review in fall of 2010. The experiences of the Austrian federation of students election can provide interesting insights for this continuous improvement process.

Bibliography

[AH04] Alvarez, R., and T. Hall. 2004. Point, click, and vote. The future of internet voting. Washington, DC.: Brookings Press.

[AH08] Alvarez, R., and T. Hall. 2008. Electronic elections. The perils and promise of digital democracy. Princeton NJ, USA: Princeton University Press.

[ASC09] Certificate according to §34 (6) HSG 1998 for the federation of students election 2009. http://www.a-sit.at/.

[BK10] Austrian Citizen Card and Specification of the Austrian Citizen Card Technology. http://www.buergerkarte.at/en/.

[BSSL01] Schneier, Bruce. 2001. Secret and Lies. IT-Sicherheit in der vernetzten Welt. dpunkt.verlag/Wiley.

[CAPA07] Parliamentary Assembly Council of Europe. 2007. Secret ballot. European code of conduct on secret balloting, including guidelines for politicians, observers and voters.

[CEIP04] Integrated Project "Making Democratic Institutions work" (2002 – 2004), Conference on The future of democracy in Europe 17-19 November 2004, Barcelona (Spain)

[CF11] Extended Validation Certificates Add Verified Identity to SSL. http://www.cabforum.org/.

[CoED04] Council of Europe. 2002-2004. Integrated Project "Making Democratic Institutions work." http://www.coe.int/t/dgap/democracy/activities/Previous%20Projects/.

[CoEO10] Council of Europe. 2010. Workshop on the "Observation of e-enabled elections", Oslo, 18-19 March. http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Evoting_Oslo_Seminar/.

[DHC06] Downs, J.S., M. B. Holbrook, and L. F. Cranor. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the SOUPS*, 79–90.

[DTH06] Dhamija, Rachna, J.D. Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the CHI*, 581–590.

[ED50] Deming, W. Edwards. Deming Circle PDCA, Presented during lectures in Japan during World War II

[EV07] Krimmer, R. 2007. *Machbarkeitsstudie. Durchführung der Hochschülerinnen- und Hochschülerschaftswahlen mittels elektronischer Abstimmungsverfahren*.

[HSG98] Federation of students law. 1998. Hochschülerinnen- und Hochschülerschaftsgesetz 1998 (HSG 1998).

[HSWO05] Election regulations. 2005. Hochschülerinnen- und Hochschülerschaftswahlordnung 2005 (HSWO 2005).

[KLSV09] Krimmer, R., C. Lehner, S. Stangl, B. Varga, R. Stein, G. Wenda, J. Kozlik 2009. E-Voting im Rahmen der Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft 2009, in Hauser, W., M. Kostal: *Hochschulrecht 09,* Wien, NWV, 539-551.

[LC10] Lehner, C. 2010. Die Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft, Doctoral Dissertation at the University of Vienna.

[LHP02] Leitold, H., A. Hollosi, and R. Posch. 2002. Security architecture of the Austrian citizen card concept. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, 391–400.

[MP08] San Martino, Antonio, and Xavier Perramon. 2008. Defending e-banking services. Antiphishing approach. Universitat Pompeu Fabra, The Second International Conference on Emerging Security Information, Systems and Technologies.

[OeH00] Head of Federation of students 2000. Statement concerning federation of students law.

[OeH07] Head of federation of students 2007. Bedenken der ÖH Bundesvertretung zu e-voting bei Hochschülerinnen- und Hochschülerschaftswahlen, September 2007

[OeW10] Informational website of the federation of students election by the election commissions. http://www.oeh-wahl.gv.at/.

[OHER10] E-Voting Evaluation Report. 2010. E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009 – Evaluierungsbericht.

[PKK04] Prosser A., R. Krimmer, and R. Kofler. 2004. Implementing an internet-vased voting system for public elections. Project experience. In *Enterprise information systems V*, ed. O. Camp, J.B.L. Filipe, S. Hammoudi, and M. Piattini, 294–299. Boston, USA/Dordrecht, Netherlands: Kluwer Academic Publishing.

[QRYM07] Qiong Ren Yi Mu Susilo, W. 2007. SEFAP. An email system for anti-phishing. In *Univ. of Wollongong, Wollongong, Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference*, 782–787.

[QSM04] Quasthoff, Matthias, Harald Sack, and Christoph Meinel. 2007. Why HTTPS is not enough. A signature-based architecture for trusted content on the social web. Hasso Plattner Institute, University of Potsdam, IEEE/WIC/ACM International Conference on Web Intelligence.

[Rec04] Council of Europe. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. https://wcd.coe.int/ViewDoc.jsp?id=778189/.

[SDOF07] Schechter S. E., R. Dhamija, A. Ozment, and I. Fischer. 2007. The emperor's new security indicators. An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the IEEE symposium on security and privacy*, 51–65.

[SLBV09] Schmidt, A., L. Langer, J. Buchmann, M. Volkamer 2009. Specification of a Voting Service Provider. In: *Requirements Engineering for E-Voting Systems (RE-VOTE).*

[Sig10] Austrian Government. Electronic signature law. Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG).

[SZKK88] Sunzu. 1988. *Die Kunst des Krieges*. Droemersche Verlagsanstalt.

[TSBA07] Trechsel, A., G. Schwerdt, F. Breuer, and M. Alvarez. 2007. *Internet voting in the March 2007 parliamentary elections in Estonia*. European University Institute. http://www.vvk.ee/public/dok/Coe_and_NEC_Report_E-voting_2007.pdf/.

[WIFE05] Whalen, T., and K. M. Inkpen. 2005. Gathering evidence. Use of visual security cues in web browsers. In *Proceedings of the conference on graphics interface*, 137–144.

[WMG06] Wu, M., R. C. Miller, and S. L. Garfinkel. 2006. Do security toolbars actually prevent phishing attacks? In *Proceedings of the CHI*, 601–610.

[XAMA05] Xenakis A., A. Macintosh 2005. Procedural Security and Social Acceptance in E-Voting. In: *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*.

[YWAP08] Yue, Chuan, and Haining Wang. 2008. Anti-phishing in offense and defense. In The College of William and Mary, annual computer security applications conference, 345–354.

Session 7: Discussion of E-Voting Protocols

Universally Verifiable Efficient Re-encryption Mixnet

Jordi Puiggalí Allepuz and Sandra Guasch Castelló

Scytl Secure Electronic Voting
Tuset 20, 1-7, 08006 Barcelona, Spain
jordi.puiggali@scytl.com, sandra.guasch@scytl.com

Abstract: Implementing a transparent audit process when an election is conducted by electronic means is of paramount importance. Universally verifiable mixnets are focused on providing such a property by means of cryptographic proofs verifiable by any auditor. While some of these systems require high amount of computing resources that make them inefficient for real elections, others proposals reduce the computation cost by sacrificing audit accuracy or reducing the voter privacy protection level. In this paper, we propose an efficient mixnet verification system that combines the advantages of the RPC and Optimistic Mixing techniques, achieving a high audit accuracy level while fully preserving voters' privacy.

1 Introduction

When developing an election by electronic means, the main problem that arises is how to implement a transparent audit process. In traditional elections, independent auditors and observers can directly oversee the election process while it is happening. An important objective of this audit process is to verify that the opening of the ballot boxes and the counting of the votes is accurately and honestly implemented. When the counting process is done by electronic means (i.e., decryption and counting of the votes), overseeing the logical process while it is executed in the machine is practically impossible: this process is a logical entity that cannot be monitored by human means as in traditional elections. Therefore, it is of paramount importance that the electronic voting system provides transparent audit means of its correct behavior.

With electronic voting, results can be verified the same way as in traditional voting: making a parallel recount of the votes. Therefore, the difficulty of the audit process relies on the proper opening of the votes: the vote decryption process.

One possible approach is to allow auditors or observers to install programs in the system to monitor the voting platform. The problem is that auditor programs should be also monitored, since the decryption process becomes also vulnerable to these programs. Therefore, the solution introduces an infinite loop that has no easy solution (who watches the watchmen?).

Alternatively, the decryption process can be audited by means of monitoring the log information generated during its execution. However, assuming that the decryption process is compromised, the log information could be also manipulated to hide any

malicious practice. Furthermore, the information provided by the decryption process should be limited, since it must preserve voter's privacy (e.g., it cannot register the relationship between a decrypted content and an encrypted vote if the later can be correlated to a voter).

In 1995, Sako and Kilian [SK95] introduced the concept of "universal verifiability" for their proposal of a vote decryption process based on a mixnet approach. This verifiability is focused on providing means for any auditor or observer to verify the correct decryption of the votes, using cryptographic proofs that are generated by the decryption process.

A mixnet or *mix network* is composed of one or various nodes that shuffle the input messages using a secret permutation. Since mix-nodes also perform a transformation process that modifies the values of the set of input encrypted votes, it is important to be able to verify the mixing and decryption procedures in such a way that privacy and integrity are preserved.

Since Chaum introduced the first mixnet in 1981 [Ch81], the search for efficient verification methods that do not break the anonymization process (i.e., revealing the secret permutation or the re-encryption factors) has been a fertile area of research. Specifically, the universal verifiability property has been the main purpose of the mixnets designed in the last fifteen years.

In this paper, we introduce a universally verifiable efficient verification method for re-encryption mixnets that achieves high correctness while preserving voters' privacy. The paper is structured as follows: in section 2 we explain our motivation to design a new mixing verification system, in section 3 the underlying cryptosystem is defined, the new verification method is presented in section 4, and the paper concludes in section 5.

2 Motivation

Providing cryptographic proofs for the universal verification of a mixing process can be complex, computationally costly, and can involve a risk of reducing the voters' privacy.

Some mixing systems ([SK95], [FS01], [Ne01]) achieve a high correctness while preserving voters' privacy at the cost of performing a great number of proofs and verifications. Since these proofs and verifications have a high computational cost, it makes them inadequate in real election environments with a large number of votes. One of the motivations for the introduction of electronic voting is to speed up the vote counting process. For this reason, there are proposals that use them to make a parallel tallying of the votes while a faster method (less accurate) is used to give faster provisional election results, as proposed in [BG02].

To improve the efficiency of the mixing process (i.e., increase the speed of the mixing and audit process), other mixing systems focused the design of their audit mechanisms on reducing the cost of their cryptographic audit mechanisms by sacrificing to some

degree the strength of the voter's privacy or reducing the accuracy of the audit process (i.e., correctness) to an acceptable level. For instance, Random Partial Checking (RPC) [JJR02] trades-off mainly privacy, while the proposal in [Go02] preserves voters' privacy, but at the expense of sacrificing some correctness and efficiency: it performs more proofs that slow down the audit process. Another method that sacrifices some privacy and correctness on behalf of efficiency is [BG02], achieving results that can be considered good enough for an electronic process when large amounts of votes are counted.

The mixing verification system presented in this paper has a high degree of efficiency (comparable to the fastest proposals) while completely preserves voter privacy, and at the same time achieves a high level of correctness for small-medium and large elections.

3 Underlying Cryptosystem

In our scheme, voters use the ElGamal cryptosystem properly parameterized for semantic security [Pf94], [TY98] to encrypt the votes. The cryptosystem is composed by three public parameters: p, q, g, a public key h, and a private key x defined in the following way:

- The modulo p is chosen as a large safe prime, that is $p=2q+1$ and q is a prime number.
- g is a generator of Gq, the q-order subgroup of Zp^*.
- The private key x is selected from Zq, and the public key h is calculated as $h=g^x \bmod p$.

In order to make the encrypted votes indistinguishable, the voting options v are configured to be all from the quadratic residue or quadratic non-residue modulo p set. In case a voting option does not fit in the set, a padding string could be added.

The voting options are encrypted using random exponents r in Zq:

$$c = (v \cdot h^r \bmod p,\ g^r \bmod p) = (c_1, c_2)$$

Therefore, an encrypted voting option can be recovered as

$$v = c_1 \cdot c_2^{-x} \bmod p.$$

There are some interesting properties of the cryptosystem that are used in our mixing verification process, such as re-encryption and homomorphic operation of the encrypted votes.

3.1 Re-encryption of the encrypted votes

Thanks to the properties of the ElGamal cryptosystem, an encrypted message can be re-encrypted using a new randomization value without changing the decryption process.

Being the encrypted vote
$c = (v \cdot h^r \bmod p, g^r \bmod p) = (c_1, c_2)$,

The re-encryption can be performed as
$c' = (c_1 \cdot h^{r'} \bmod p, c_2 \cdot g^{r'} \bmod p) = (v \cdot h^{r+r'} \bmod p, g^{r+r'} \bmod p) = (c_1', c_2')$.

The re-encrypted vote can be decrypted as usual:
$v = c_1' \cdot c_2'^{-x} \bmod p$.

3.2 Homomorphic operation of the encrypted votes

Being two votes v_1 and v_2, an encryption operation E, and two algebraic operations Φ and Θ, the homomorphic property can be defined as
$E(v_1) \, \Phi \, E(v_2) = E(v_1 \, \Theta \, v_2)$.

Since ElGamal is a cryptosystem with homomorphic properties, the product of n encrypted votes c_i generates an equivalent encrypted information Ec whose content Ev is the product of the plaintext voting options and the encryption exponent r_e is the sum of the individual encryption exponents:

$$\prod_{i=1}^{n} c_i = (\prod_{i=1}^{n} v_i \cdot h^{r_i}, \prod_{i=1}^{n} g^{r_i}) = ((\prod_{i=1}^{n} v_i) \cdot h^{\sum_{i=1}^{n} r_i}, g^{\sum_{i=1}^{n} r_i}) =$$
$$= (Ev \cdot h^{r_e}, g^{r_e}) = Ec$$

4 Mixing process and verification

4.1 Overview

The universal verification method for re-encryption mixnets presented in this paper combines the advantages of the RPC technique [JJR02] and the "Optimistic Mixing" proposal [Go02]: the partial disclosure of information is combined with proofs calculated from homomorphically aggregated groups of votes to achieve greater levels of privacy, robustness and soundness than these methods.

In the first step, each mix-node shuffles and re-encrypts the input encrypted votes, storing in a secret and secure way the permutation and re-encryption values applied for each vote. When the last node has mixed and re-encrypted its inputs the anonymized votes are ready to be decrypted, but before disclosing any significant information, the correct performance of the mixnet is universally verified.

In the verification process, the input encrypted votes of each node are divided into several independent groups following a random organization proposed by a verifier (i.e., an auditor). As said before, this group organization is done at the end of the mixing process (i.e., before decrypting the votes), preventing the disclosure of sensitive

information to any mixing node in order to cheat the verification process. Then each prover—the mix-node—provides information to the verifier about the global location in the mix-node's output of the votes belonging to each group in the input.

The global location of the votes of one output group does not disclose the individual position of each vote related to its original input group in the mix-node. For instance, disclosed output group positions are sorted by numerical value instead of their position in the mix-net input group.

When the verifier divides the input encrypted votes into groups, it also multiplies the votes in each group to obtain an *Input Integrity Proof* using the homomorphic properties explained in section 3.2. After the prover indicates which votes in the output of the node belong to each input group, the verifier can multiply the votes belonging to each output group to obtain an *Output Integrity Proof*. For each pair *Input-Output Integrity Proof* at each node, the prover provides a Zero-Knowledge Proof to demonstrate that the *Output Integrity Proof* is the re-encryption of the *Input Integrity Proof*.

Since the integrity proofs can be calculated and verified by any auditor, this method achieves the universal verifiability objectives. Furthermore, this proposal allows the verification of the mixing process without disclosing information about the position of individual votes in the output node after the shuffling process, preserving voters' privacy.

The next sections provide the details of vote group generation, the integrity proofs, and their related ZKPs.

4.2 Creating the groups

When the verification process starts, the verifier randomly defines how the input votes in the first mix-node are grouped by sending an array with the indexes of the position of the votes to be grouped:

For m input votes: $\{v_1, v_2, v_3, ..., v_m\}$.
An example of a grouping array is: $\{v_3, v_{m-1}, v_5, ..., v_2\}$.

Since the size of the groups is pre-defined (explained at the end of this section), the prover organizes the input votes following the grouping array order to define each vote group contents. Then, using the mixing permutation information, the prover indicates to the verifier for each mix-node output vote the group to which it belongs to. Since this information is provided following the order of the mix-node output votes, it is not possible to individually correlate input and output votes (only group affiliation).
For the next nodes of the mixnet, input vote groups are re-defined using as reference the output vote groups of the previous mix-node. We do not propose the reorganization of the groups at random, as in the first mix-node, to prevent disclosing information that could be used to correlate mixnet last output votes with first input ones: an attacker could analyze the votes belonging to each new grouping at each mix-node and identify

intersections of the groups that could facilitate the tracing of output votes with a reduced set of input votes (or in the worst case, an individual vote) of the fist mix-node. If so, the probability of an input vote being connected to a specific final output vote would be different from *1/m*, opening the door to privacy issues.

In order to prevent this attack, the new input groups are created by taking votes from different output groups of the previous mix-node. This is done in such a way that the groups in the last mix-node are composed of at least one vote from each group defined in the first mix-node. A proposal to redefine the groups consists of creating a new group by selecting votes belonging to different groups in the previous node in a consecutive way, like it is shown in figure 3. In this figure, the first group of the second node (G1,2) is formed by a vote from the first group of the first node (G1) and by one of the second (G2); the group of the second node (G3,4) is formed by a vote of the third group of the first node (G3) and one of the fourth (G4), and so on.

In order to preserve voter privacy, the size of the group also matters (e.g., if the size of the groups is too small, maybe the votes are not equally distributed at the last node of the mixnet). Furthermore, the probability of detecting manipulations of the votes during the mixing process also depends on the size of the groups (the smaller the group is, the higher the probability of detecting the manipulation of any vote is). For this reason, the groups need to be set up in a proper way to achieve the highest detection ratio without compromising voter privacy.

Being t the number of mixnet nodes (at least two) and m the total number of votes, the number of n votes inside a group should be at least:

$$n = \sqrt[t]{m} \qquad [1]$$

This formula preserves the privacy and optimizes manipulation detection rates of the votes. As shown in the formula, in our proposal the number of mixnet nodes also contributes to the correctness of the verification process. However, this optimization should be evaluated carefully, since the addition of new mixnet nodes reduces the efficiency of the proposal: increases the number of cryptographic operations required by the mixing and verification processes.

In the possible case of one or more nodes disclosing information about the individual permutations applied to the votes, they would not be taken into account in the formula 1. Therefore, privacy would still be maintained.

4.3 Generation of the ZKP of the Integrity Proofs

The integrity check of the votes grouped at each node is based in the homomorphic properties of the ElGamal encryption scheme. We call the result of multiplying a group of votes *Integrity Proof.*

The result of the multiplication of *n* votes of the same group in the input of a node, or *Input Integrity Proof* can be defined as:

$$\prod_{i=1}^{n} c_i = (\prod_{i=1}^{n} v_i \cdot h^{r_i}, \prod_{i=1}^{n} g^{r_i}) = ((\prod_{i=1}^{n} v_i) \cdot h^{\sum_{i=1}^{n} r_i}, g^{\sum_{i=1}^{n} r_i}) = (Ev \cdot h^{r_e}, g^{r_e})$$

The multiplication of the same group of votes in the output of the node (i.e., the same votes after being re-encrypted), is called *Output Integrity Proof* and it is equal to:

$$\prod_{i=1}^{n} c_i' = (\prod_{i=1}^{n} v_i \cdot h^{r_i + r_i'}, \prod_{i=1}^{n} g^{r_i + r_i'}) = ((\prod_{i=1}^{n} v_i) \cdot h^{\sum_{i=1}^{n} r_i + r_i'}, g^{\sum_{i=1}^{n} r_i + r_i'}) =$$
$$= (Ev \cdot h^{r_e + r_e'}, g^{r_e + r_e'})$$

Since the mix-node knows all the individual re-encryption factors of the votes of each group, it can calculate the accumulated re-encryption factor $r_e' = \sum_{i=1}^{n} r_i'$. Having this accumulated factor, the mix-node can make a Non-Interactive Zero Knowledge Proof of Re-encryption (NIZKP-RE), proving that the *Output Integrity Proof* is the re-encryption of the *Input Integrity Proof* using the re-encryption factor r_e‘ . This proof can be based on the Schnorr Identification Protocol like in [MA99] or the Chaum-Pedersen proof of equality of discrete logarithms [CP93].

Therefore, any auditor, after calculating by herself the *Input Integrity Proof* and *Output Integrity Proof* of the groups of a node, can use the NIZKP-RE to check that both proofs are based on the same contents. In other words, the global contents of the votes in a group still remain the same. Since the integrity proofs are based on the homomorphic product of the votes, there is still a possibility that a rogue mix-node could cheat the system. However, as explained in section 4.5.1, the way the groups are modeled in our proposal makes the probability of detecting such manipulation very high (e.g., it has a probability of 99.91% of detecting a manipulation of 2 votes in an election with 10,000 votes).

If the proof is successfully verified, the node is believed to behave correctly. This NIZKP-RE is done for each group of votes at each node.

4.4 Verification Protocol Summary

To summarize, the verification protocol implements the following steps after the mixing process:

1. For the first mix-node, the verifier divides at random the input votes in groups using a grouping array that is sent to the prover.
2. Then, the verifier calculates an *Input Integrity Proof* for each group.

3. The verifier asks the prover for the output destination of the votes belonging to each group and calculates an *Output Integrity Proof* for each group.
4. The prover calculates a NIZKP based on the re-encryption factor in order to demonstrate that the *Output Integrity Proof* is the re-encryption of the *Input Integrity Proof* of the same group.
5. For the next node, the groups are redefined in such a way that each new group is composed of votes from different output groups in the previous node, and the steps 2–5 are repeated until the correct behavior of the last mix-node is verified.

An example of the procedure is shown in Fig. 1. The figure also shows the group configuration at each mix-node:

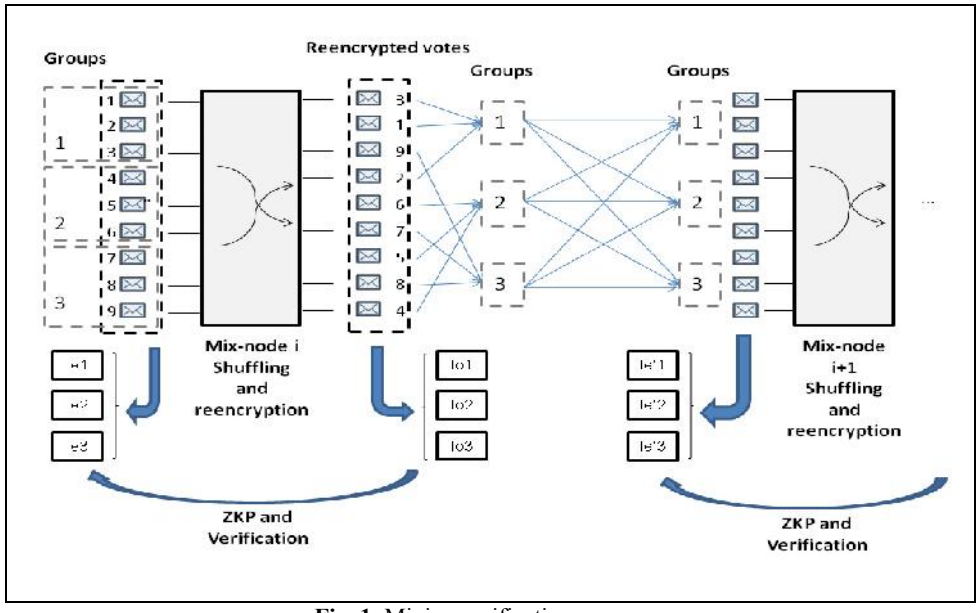


Fig. 1: Mixing verification process

4.5 Properties of the new system

We analyze the new verification method proposed from four points of view: soundness, efficiency, privacy, and universal verifiability.

4.5.1 Soundness

Since the verification process is based on the *Integrity Proofs* that are calculated by multiplying groups of votes, an attacker could take advantage of the cryptosystem's homomorphic properties in order to modify the votes in the mixnet without being detected. In fact, if several votes in the same group are modified in such a way that the

modifications are cancelled when the *Integrity Proof* is calculated, these changes are not detected in the verification process. However, since the group configuration is unknown until the mixing process finishes, the probability of an attacker changing a significant amount of votes without being detected is negligible.

The chance of an attacker not being detected depends on the amount of votes in the mixnet, the number of groups in which the votes are divided, and the number of manipulated votes. Since the probability of being undetected decreases with the number of modified votes, we can define the most successful scenario for the attacker as the one where only two votes are manipulated, they are in the same group, and the modifications cancel out when the *Integrity Proof* is calculated.

The probability of detecting a pair of manipulated votes is:

$$P_{success} = 1 - \frac{n-1}{m-1}, \qquad [2]$$

where m is the total number of votes and n is the number of votes in each group.

It is important to maintain a convenient relationship between the total number of votes processed by the mixnet and the size of the groups: the smaller the groups are, the higher the probability of detecting an attacker is. Otherwise, the larger the groups are, the faster the verification process becomes.

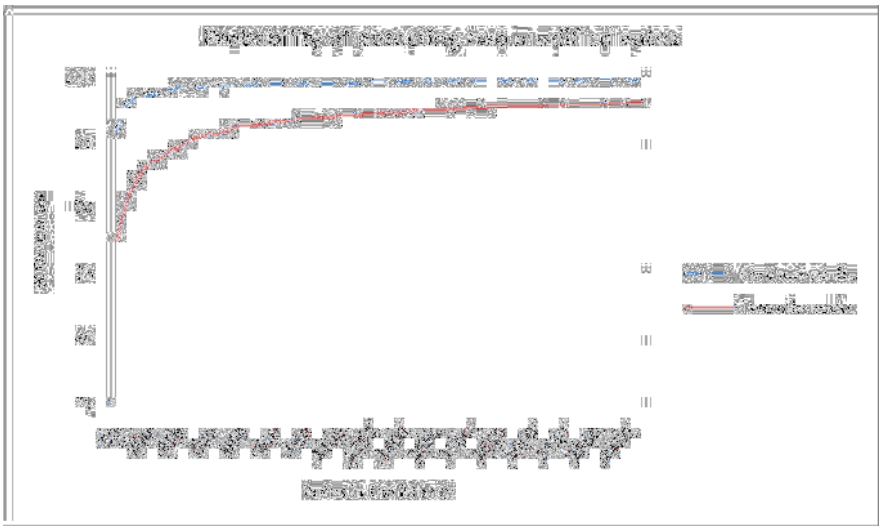


Fig. 2: Graphic showing the probability of detecting two modified votes when two mix-nodes and four mix-nodes are used.

Formula 1 gives an optimized relationship between the size of a group of votes and the total number of votes that are processed by the mixnet to meet the efficiency, soundness, and privacy requirements.

For example, in an election with 10,000 votes and a mixing of two nodes, the minimum size of the groups in order to preserve the voter privacy is 100 votes. With this configuration the probability of detection of two modified votes is 99%. If the mixing is performed with four nodes, the minimum size for each group is ten votes, which gives a probability of detection of 99.91%.

The probability of detecting two modified votes in a mixnet composed of two mix-nodes (bigger groups) or of four mix-nodes (smaller groups) is shown in Fig. 2. In both cases the probability of detection tends toward 100%, but when more mix-nodes are used and smaller groups are configured, the probability of detection increases faster.

4.5.2 Privacy

Following the procedure described in section 4.2., groups at the input of each node contain votes from different groups of the previous node's output, in such a way that it is impossible for an attacker to track back the output votes to the groups defined in the first mix-node. Therefore, the privacy level of the verification method does not compromise the original privacy provided by the re-encryption mixnet.

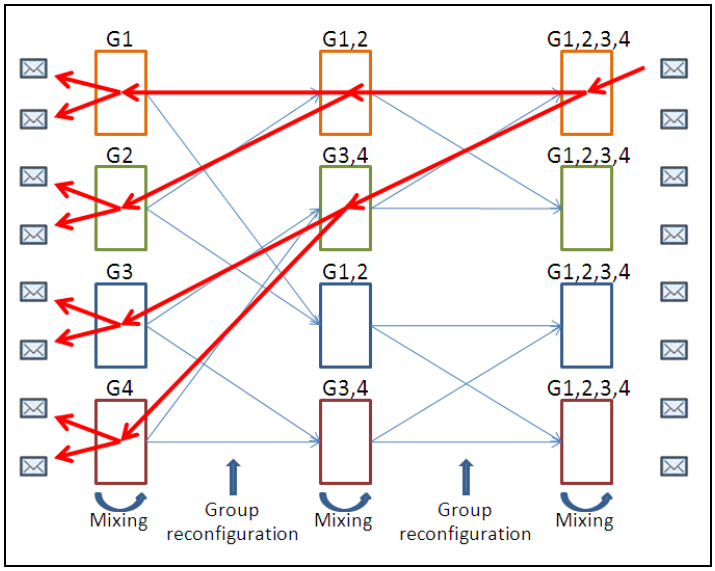


Fig. 3: Traceability of a message in the mixnet.

Fig. 3 shows how privacy is maintained due to the group reconfiguration at each node. An attacker choosing any encrypted vote of the mixnet output cannot successfully track it back to an individual encrypted vote in the input or any subset of input votes.

Therefore, all the votes in the input have the same probability of being in a specific output.

Formula 1 defines the group size depending on the number of mix-nodes for a fixed amount of votes in the mixnet. In the case that it is desirable to use small groups to increase the probability of detecting manipulated votes (the soundness of the proofs), more nodes in the mixnet are needed to preserve voter privacy.

4.5.3 Efficiency

Preserving voters' privacy and audit soundness by dividing the votes into small non-overlapping groups has an odd behavior: it reduces the efficiency of the mixnet. The computation costs of the verification method depend on the number of votes in the system and the amount of groups created for the verification process, since the proofs of correct behavior are done over them. Therefore, for a fixed number of votes in the mixnet, the more groups there are, the more the computation costs are consumed. On the other hand, the probability of detecting manipulated votes increases since there are less votes in each group.

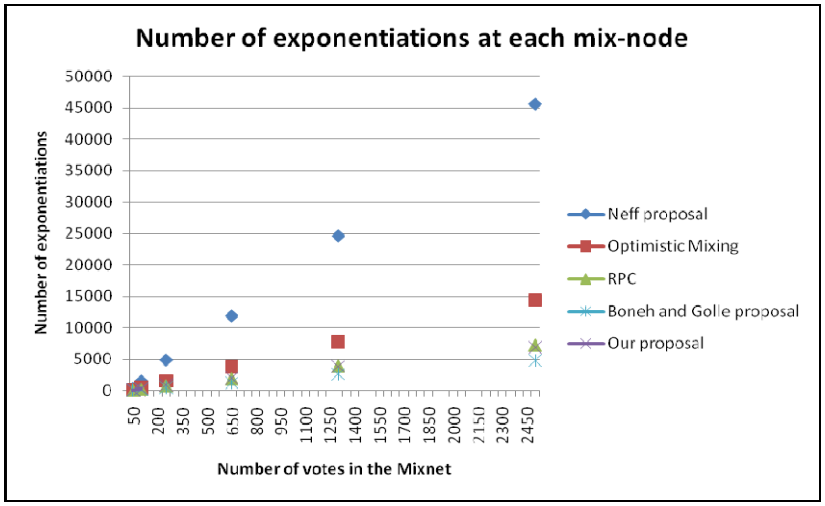


Fig. 4: Comparison of the number of exponentiations required at each mix-node in some mixing verification systems

We have estimated the cost of performance of our method based on the number of exponentiations done at each phase:

- Mixing: the re-encryption of the votes at each mix-node requires $2m$ exponentiations, where m is the total number of votes in the mixing.
- Proof of correct mixing: calculating the zero-knowledge proofs of correct performance at each node requires $2(m/n)$ exponentiations, where (m/n) is the

number of groups in which the total number of votes is divided at each node, and *n* is the number of votes per group.
- Verifying correct mixing: the verification of correct mixing at each node requires 4*(m/n)* exponentiations.

In the Fig. 4, a comparison of our method with other mixing verification systems in terms of the number of exponentiations is provided, showing that our system is one of the fastest for large amounts of votes.

4.5.4 Universal verifiability

A universally verifiable mixnet provides a proof of correct mixing that any observer can verify. For this purpose, some information is stored to let any auditor check the verification process after the mixing. Since the verification is made in zero knowledge, there is no need for the auditor to have any special or private data (i.e., private key of the election) to perform this check. The information collected during the mixing process for further verification consists of the set of encrypted votes in the mixing input and the re-encrypted votes at the output of each mix-node. During the verification process, the configuration of the votes in (input/output) groups and the zero-knowledge proofs performed by each node are also stored. Therefore, any auditor can check the verification process later using this information: the *Input* and *Output Integrity Proofs* can be calculated from the input/output sets at each node and the zero-knowledge proofs between them can be verified.

5 Conclusions

In this paper we described a new proposal of a universally verifiable and efficient method for re-encryption mixnets that achieves high correctness while preserving voters' privacy. Specifically, our proposal achieves an efficiency level comparable to the current faster existing systems, while our capacity of detecting manipulated votes is closer to the most accurate methods without compromising the voters' privacy.

Assuming an implementation of four nodes and setting the vote group size of the verification process to optimize the relationship between full voter privacy, efficiency, and fraud detection (using the formula 1 described in section 4.2), we can achieve the following conclusions.

From the point of view of efficiency, the computation cost of our proposal is close to the Boneh and Golle method [BG02]: the fastest one as shown in the figure 4. Regarding RPC method [JJR02], this is more efficient only for small batches of votes (less than 1500), but when the amount of votes increases, our system becomes faster. Considering the other methods [Go02][Ne01], the efficiency improvements are clear.

In terms of privacy, compared with our proposal, the original RPC proposal offers a weaker privacy level, since the input votes could be connected with some specific output

votes with a probability higher than *1/m*. An improvement proposed by Chaum [Ch02] solves this privacy issue by grouping pairs of mix-nodes in a special way during the verification and requiring at least four nodes. However, the problem still remains if the information from intermediate nodes is disclosed. On the other hand, in the method explained in [BG02], full voter privacy is difficult to achieve: each verification round done to increase the accuracy of the verification process discloses sensitive information that could be used to increase the probability of correlating input and output votes. In our proposal, we keep full voter privacy.

In terms of accuracy, our proposal achieves a high level of cheating detection for a small number of manipulated votes (i.e., 2 votes). This probability is closer to 100% when the number of votes is near 300 votes (99%). The other methods, except [Ne01], have similar or lower accuracy levels.

In summary, compared with the current verification methods, our solution is the most well-balanced in terms of efficiency, privacy, and accuracy, while providing universal verification properties.

Bibliography

[BG02] Boneh, D., and P. Golle. 2002. Almost entirely correct mixing with applications to voting. In *Proceedings of the 9th ACM conference on computer and communications security (Washington, DC, USA, November 18–22, 2002) CCS '02*, ed. V. Atluri, 68-77. New York NY: ACM.

[Ch02] Chaum, D. Secret ballot receipts and transparent integrity. Better and less-costly electronic voting at polling places.White Paper. http://www.vreceipt.com/article.pdf/.

[Ch81] Chaum, D. L. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM 24*, 2 (February): 84-90.

[CP93] Chaum, D., and T. P. Pedersen. 1993. Wallet databases with observers. In *Proceedings of the 12th annual international cryptology conference on advances in cryptology (August 16–20, 1992). Lecture notes in computer science, vol. 740*,ed. E. F. Brickell, 89–105. London: Springer-Verlag.

[FS01] Furukawa, J., and K. Sako. 2001. An efficient scheme for proving a shuffle. In *Proceedings of the 21st annual international cryptology conference on advances in cryptology (August 19 - 23, 2001). Lecture notes in computer science, vol. 2139.* ed. J. Kilian, 368–387. London: Springer-Verlag.

[Go02] Golle, P., S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. 2002. Optimistic mixing for exit-polls. In *Proceedings of the 8th international conference on the theory and application of cryptology and information Security. Advances in cryptology (December 01 - 05, 2002). Lecture notes in computer science, vol. 2501,* ed. Y. Zheng, 451–465. London: Springer-Verlag.

[JJR02] Jakobsson, M., A. Juels, and R. L. Rivest. 2002. Making mix nets robust for electronic voting by randomized partial checking. In *Proceedings of the 11th USENIX security symposium (August 05–09, 2002). USENIX Security Symposium,* ed. D. Boneh, 339–353. Berkeley CA, USA: USENIX Association.

[MA99] Markus, J., and J. Ari. 1999 *Millimix. Mixing in small batches*. Technical Report 99-33. Center for Discrete Mathematics & Theoretical Computer Science.

[Ne01] Neff, C. A. 2001. A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM conference on computer and communications security (Philadelphia, PA, USA, November 05 - 08, 2001). CCS '01*, ed. P. Samarati, 116–125. New York, NY: ACM.

[Pf94] Pfitzmann, B. 1994. Breaking efficient anonymous channel. In *Advances in cryptology (Eurocrypt '94), volume 950 of LNCS*, ed. A. D. Santis, 332–340. Berlin: Springer-Verlag.

[SK95] Sako, K., and J. Kilian. 1995. Receipt-free mix-type voting scheme. A practical solution to the implementation of a voting booth. In *Advances in cryptology - EUROCRYPT '95. Lecture notes in computer science*, ed. C. Guillou and J. Quisquater, 393-403. Berlin: Springer-Verlag.

[TY98] Tsiounis, Y. and M. Yung. 1998. On the security of ElGamal based encryption. In *Proceedings of the first international workshop on practice and theory in public key cryptography. Public key cryptography (February 05 - 06, 1998). Lecture notes In computer science, vol. 1431*. ed. H. Imai and Y. Zheng, 117–134. London: Springer-Verlag.

Why Public Registration Boards are Required in E-Voting Systems Based on Threshold Blind Signature Protocols

Reto E. Koenig[1], Eric Dubuis[2], Rolf Haenni[2]

[1]University of Fribourg
Department of Computer Science
CH-1700 Fribourg, Switzerland
reto.koenig@unifr.ch

[2]Research Institute for Security in the Information Society
Bern University of Applied Sciences
Quellgasse 21, Postfach
CH-2501 Biel, Switzerland
{eric.dubuis,rolf.haenni}@bfh.ch

Abstract: In this paper, we demonstrate that e-voting protocols based on threshold blind signatures from multiple authorities allow a coalition of m eligible voters to cast more than m votes. This property presents a serious violation of the principles of democracy in the voting process. We analyze the applicability of this violation and provide a generic solution using a public registration board and modified threshold signature schemes.

1 Introduction

Threshold blind signature schemes provide several highly desired properties in cryptography: privacy, security, robustness through redundancy, and avoidance of single points of failure. Many existing threshold blind signature schemes allow independent signature requests from multiple signers, i.e., no communication among the signers has to take place. Exactly this property applied in an e-voting protocol results in a severe violation of the principles of democracy in the voting process. To the best of our knowledge, no protocol design based on threshold blind signature has ever been analyzed regarding this fact.

1.1 Related Work

One of the central technical challenges of designing an e-voting protocol is to simultaneously authenticate voters unequivocally while preserving the anonymity of their votes. One approach is to define the system based on *blind signatures* [Ch82], [Ch83]. The development of such systems is stimulated by the fact that blind signature schemes are simple to understand and implement, flexible enough to be adjusted to all sorts of settings, and suitable for large-scale elections.

Applying blind signatures to e-voting was first proposed in [FOO92]. In the suggested protocol, known as FOO92, the voter first encrypts the vote and then requests a blind signature from the voting authority. The blind signature ensures that the content of the vote remains entirely disguised from the voting authority during the authorization process. The encrypted vote, together with the blind signature, is then sent over an anonymous channel to a public board. To open the votes for counting, the voter supplies the encryption key at the end of the voting period, again over an anonymous channel.

One of the major drawbacks of FOO92 is its potential for single points of failure, e.g., it allows the authority to introduce votes for voters who abstain from casting their votes. This and other drawbacks have been addressed in the literature, and hence, many variations of the FOO92 protocol exist today [CC96], [Ok97], [Ba94], [Oh99], [RRN01], [CC97], and [He97].

One aspect, which is common for presentday protocols, is the replication of entities having the property of single point of failure. This replication allows the distribution of power as only a certain number of instances is needed in order to keep the protocol from failing, see for example [Du99], [Ki02], [JZF03], [Ba0], [AFT07], [AW07], and [CCM08].

1.2 Contribution and Overview

In Section 2, we will briefly illustrate the above-mentioned class of protocols. We will demonstrating a generic e-voting protocol based on threshold blind signature, where entities with the property of single point of failure are replicated. We will then analyze the attack on the provided generic scheme where any coalition of m eligible voters can cast more than m votes. Our analysis will provide us with some qualitative and quantitative results.

In Section 3, we present a generic counter-measure against the above-mentioned attack, which is applicable to many existing e-voting schemes of that class. Section 4 gives a security analysis on the revisions made in Section 3, and Section 5 provides our conclusions.

2 E-Voting Protocol using Threshold Blind Signature Scheme

In the following we present a generic template e-voting protocol using threshold blind signatures. This protocol shall serve as the representative for various state-of-the-art e-voting protocols of this class. For the sake of readability, certain aspects of the protocol will be omitted whereas a more detailed view will follow in a proceeding section. Even though other protocols are different in detail, they carry the same threshold properties.

2.1 Threshold Blind Signature

To avoid an entity becoming a single point of failure, the entity is replicated N times where it is assumed that at least t replicates work in the sense of the protocol. The threshold t must be greater than 1 and smaller than N. To maximize the robustness and reliability of the protocol, the choice of t should make it unlikely that t or more replicates of an entity collude, or that $N - t$ replicates fail. For e-voting protocols, $\frac{2}{3}N \leq t \leq \frac{3}{4}N$ is often mentioned as a reasonable choice in multi-party computation [Hi01].

Concrete Examples of Blind Signature Schemes

RSA Based Blind Signature. A *blind signature*, as introduced by Chaum [Ch82], is a form of digital signature, where the signer A is not supposed to see the real message to be signed, nor can the signer trace back the signature to the voter V (i.e., an unknown signature to an unknown message for a known requester). In order to achieve this goal, the data x to be signed is disguised before it is given to the signer using a blinding function. This function usually involves a public key e of the signer and a random number r:

1. $V \rightarrow A: x' = \text{blind}_e(x, r)$.

After the signer has signed the blinded data x' with the private key d, the resulting blind signature s' can be transformed into an ordinary digital signature s using a corresponding unblinding function:

2. $A \rightarrow V: s' = \text{sign}_d(x')$,
3. $A: s = \text{unblind}(s', r)$.

In the classical RSA scheme, the blinding and unblinding functions consist of multiplying x with the blinding factor r^e and s' with the unblinding factor r^{-1}, respectively.

Schnorr Based Blind Signature. Blind signature schemes based on discrete logarithms were first introduced by Schnorr [Sc90]. In this scheme, the blinding and unblinding function consists of a typical Σ communication scheme:

1. $A \rightarrow V: r' = g^k \bmod p$, where $k \in_R Z_q$, $e = g^{-c} \bmod p$, and g, p, q are setup parameters.
2. $V \rightarrow A: x' = \varepsilon - \beta$ where $\varepsilon = H(x, r)$, $r = r' g^{\alpha} e^{\beta} \bmod p$, and $\alpha, \beta \in_R Z_q$.
3. $A \rightarrow V: s'_i = k + x'c \bmod q$.

The resulting blind signature (r, s') for the blinded data x' can be transformed to a signature (r, s) for the data x by applying the corresponding unblinding function $s = s' + \alpha \bmod q$.

Threshold Blind Signatures

A *threshold blind signature* scheme is a combination of a threshold signature scheme with blind signatures such that the data to be signed is not revealed to the signers, nor can the signers trace back the signature to the corresponding voter.

A threshold blind signature scheme can be defined as a (t, N)-*threshold signature* scheme. This scheme lets N parties sign some common data, such that the outcome is a valid signature, if at least t parties have contributed to the signature [Bo03]. We can simply realize such a scheme by having each party sign the data x individually and then count the number of valid signatures, in order to decide if the threshold has been reached. In the following we will use a generic description of blind signatures which can be adapted to any blind signature scheme: If $\mathbf{s} = (s_1, \ldots, s_k)$ with $t \leq k \leq N$ denotes the individual signatures and $\mathbf{e} = (e_1, \ldots, e_N)$ the public keys of the signers, we denote the corresponding verification function by

$$\text{verify}_{\mathbf{e},t}(\mathbf{s}, x) \in \{true, false\}.$$

2.2 The Protocol

The common e-voting protocol for such systems involves five entity types (voter, administration, the registration authority, the key authority, voting board) and consists of five consecutive phases:

Phase 1: Initialization. The administration initiates the voting process by distributing the empty ballots, and the set of identities of legitimate voters together with their public keys to all necessary entities.

The key authorities create the public-key / secret-key pair for a randomized asymmetric cryptography used during the voting process. In order to dissolve power, the key generation process is done in a distributed way, by using a threshold scheme such as [Ge03] whose description is beyond the scope of this paper.

Phase 2: Voter Preparation The voter fills in the empty ballot and randomly encrypts the resulting vote by the public key provided by the key authorities. The resulting message is called the vote. At the end of this phase, the voter is ready to start the registration process.

Phase 3: Registration The purpose of the registration phase is to authorize legitimate voters to cast their votes. For this, the voter requests a signature for the blinded vote from at least $t \leq N$ registration authorities. The blinding of the vote has to be generated for each replicated registration authority separately, as each replicate uses its own private key for signing. The voter sends the blinded vote to each registration authority where it will be signed and returned if and only if the following two conditions hold: The voter is allowed to vote, and the voter has not previously requested another signature during the

voting process. Upon reception, the voter obtains the signatures for the vote by unblinding. If at least t signatures have been received then the voter is ready to start the vote casting process.

Phase 4: Vote Casting The voter sends the vote together with the authorities' signatures anonymously to the public voting board. The board accepts the vote if and only if there are at least t valid signatures associated to it.

Phase 5: Counting The last phase of the e-voting protocol involves the opening of the votes to make them available for counting. For this, the key authorities publicly decrypt the cast votes using the secret part of the key pair. The votes are now ready to be counted by everyone.[1]

2.3 Violation of Democracy

We will now demonstrate the attack on democracy by exploiting the properties of the described threshold blind signature protocols.[2]

Definition 1 (Democracy) A system is democratic if authorized voters can vote (*eligibility*), and if eligible voters can vote only once (*uniqueness*).

Let us first analyze Phase-3 in more detail where the voter has to address a signing request to at least t replicates of the registration authority. The voter generates a blinded message for each signer, whereas each blinded message consists of the same vote. Each signer will sign the received message and returns it to the voter. The vote will be declared valid if at least t different and valid signatures for the vote are provided.

This protocol implicitly violates democracy and therefore can be used as an attack on the e-voting system. As only t signatures are needed in order to render a vote valid, $N - t$ signatures can be used for another vote. One voter cannot get more than one valid vote, but a group of voters can. The following example shall demonstrate a possible attack:

- available registration authorities: $N = 4$
- authority signature threshold: $t = 3$

A *fair* voter V_i generates four blinded messages (one blinded message w'_{ji} per authority A_j, $1 \leq j \leq 4$) containing the same vote w_i:

	A_1	A_2	A_3	A_4
V_i	w'_{1i}	w'_{2i}	w'_{3i}	w'_{4i}

[1] This phase can be adapted in manifold ways, such as re-encryption to gain receipt freeness or homomorphic counting instead of individual decryption. Since these adoptions distract from the intended focus of this paper and, hence, will not be followed any further.

[2] Many to our colleague Emmanuel Benoist for pointing this out.

Each authority signs the blinded message and returns the signature s_{ji}' to the voter. To cast the vote w_i, the voter sends it together with three out of four unblinded signatures s_{ji} anonymously to the voting board. The voter discards the remaining signature.

A *malicious voter group* consisting of three colluding voters V_k, V_l, V_m, where $k, l, m \in \{1, \dots, N\}$ and $k \neq l \neq m$ can generate an additional vote w_x resulting in four independent votes:

	A_1	A_2	A_3	A_4
V_k	w'_{1k}	w'_{2k}	w'_{3k}	w'_{4x}
V_l	w'_{1l}	w'_{2l}	w'_{3x}	w'_{4l}
V_m	w'_{1m}	w'_{2x}	w'_{3m}	w'_{4m}

The following holds true:

- w_k is rendered valid by the signatures s_{1k}, s_{2k}, s_{3k} of authorities A_1, A_2, and A_3;
- w_l is rendered valid by the signatures s_{1l}, s_{2l}, s_{4l} of authorities A_1, A_2, and A_4;
- w_m is rendered valid by the signatures s_{1m}, s_{3m}, s_{4m} of authorities A_1, A_3, and A_4; and
- w_x is rendered valid by the signatures s_{2x}, s_{3x}, s_{4x} of authorities A_2, A_3, and A_4.

This is possible as the different registration authorities operate independently from each other and, hence, no synchronization takes place amongst them. Even though the attack is not possible on an exponential scale, it is still significant. The quantitative impact of the attack is proportional to the number of colluding voters.

Due to the nature of threshold there always exists a subset of size $N - t$ authorities not needed in order to get sufficient signatures for a valid vote. Let V_c be the size of a malicious colluding voter group. Hence, the maximum number of additional votes v_+ that can be rendered valid by the malicious voter group, is:

$$v_+ = \left\lfloor \frac{N - t}{t} V_c \right\rfloor$$

For the threshold values N, t such that $\frac{2}{3}N \leq t \leq \frac{3}{4}N$ (see Section 2.1), v_+ is in the range of:

$$\frac{V_c}{3} \leq v_+ \leq \frac{V_c}{2}$$

The violation of democracy shown above is present in all protocols based on threshold blind signature where the blinding procedure results in a different message for every individual signer. Therefore, a common registration board must be used as knowledge base for synchronization amongst the registration authorities.

3 E-Voting Protocol Using a Public Registration Board

A public board is a broadcast channel with memory. Data can be broadcast by anyone. By using a guard,[3] the accepted data can be restricted to authorized participants only. Once published, the data can be read by everyone but cannot be altered anymore. The concept of the public board has been introduced by Benaloh et al. [CF85] and [Be87] and brings verifiability to e-voting schemes.

To prevent the violation of democracy, we introduce a public registration board. We assume that the guard of the board guarantees the following properties:

- Only eligible voters can append an entry (using the public key for identification).
- Each eligible voter can append only once.
- Only eligible registration authorities can append signatures (using the public key for identification).
- Each eligible registration authority can append only one signature per eligible voter entry.

3.1 Revised Voting Protocol

By introducing a public board for the registration process, the voter no longer communicates to the registration authorities. Instead, the blinded hash of the encrypted vote is broadcast to the public registration board. In addition, the registration authorities no longer communicate to the voters. Instead, the registration authorities read the public registration board entries and broadcast the signed voter entries back to it. Therefore, the initial Phase 3 of the generic protocol in Section 2.3 needs the following revision:

Phase 3: Registration The purpose of the registration phase is to authorize legitimate voters to cast only their votes. For this, the voter requests a signature for the blinded hash of the encrypted vote from at least $t \leq N$ registration authorities. The voter does so by broadcasting the blinded hash of the encrypted vote along with the public voter key to the public registration board. The registration board will accept the message if and only if the following two conditions hold: The voter is allowed to vote, and the voter has not yet requested another signature during the voting process. These conditions also prevent the public registration board from being flooded. Each registration authority will sign one blinded hash per voter and broadcasts this signature back to the public registration board. Then, the voter can obtain the signatures for the hash by unblinding them. If at least t signatures have been added to the public registration board then the voter is ready to start the vote casting process.

[3] A guard is a predicate on a candidate entry and on the board's state. The predicate must evaluate to true for the entry being added to the board. If the predicate evaluates to true then we call the candidate entry to be *valid*, and it is added. Otherwise, if the predicate evaluates to false then the candidate entry is discarded.

The following revision of the Phase 4 prevents the board from being flooded:
Phase 4: Vote Casting The voter sends the encrypted vote, the vote hash, and the authorities' signatures anonymously to the voting board. The board accepts the vote if and only if there are at least t valid signatures associated to the vote hash.

3.2 Public Registration Board Collective

The public registration board presented at the beginning of Section 3 may suffer from some catastrophic failure that prohibits it from fulfilling its duty. It may no longer be able to service its regular clients, or it may be victim of a denial of service attack, with the same effect that prevents regular clients to communicate successfully with the board.

In [HL09], a scheme for a collective of public boards is presented being based on N *peers* of identical public boards. As long as a threshold set of t out of N public boards function correctly, the integrity of the entries on the boards can be guaranteed by the collective. Each peer accepts and stores the same information as outlined in the beginning of Section 3. In order to write information onto the board, voters and authorities send their messages to one peer of their choice. The peer in turn will then form a threshold set t of peers to guarantee (in terms of a receipt) the publishing of the message.

There are two versions of the collective: The first one having a *synchronized history*, all peers maintain the same order among the accepted messages. The second version supports the concept of an *unsynchronized history* which satisfies our requirements. To read all messages previously published, however, clients need to consult $N - t + 1$ peers.

3.3 Revised Threshold Blind Signature Schemes

The revision of Phase-3 requires a property which is not present in the normal schemes as defined in Section-2.1. It requires that each signing party (registration authority) is given the *same* blinded data x' such that the very same data is signed by all parties. Therefore, a new assumption has to be introduced: The blinding and the unblinding function,

$$x' = \mathrm{blind}_{\mathbf{e}}(x, r),$$
$$\mathbf{s} = \mathrm{unblind}_{\mathbf{e}}(\mathbf{s}', r),$$

depend on the public keys $\mathbf{e}$ of all signing parties.

RSA Based Threshold Blind Signature

To realize such a scheme based on RSA, we use a common blinding factor $r^{e_1 \cdots e_N}$ and individual unblinding factors $r^{-(e_1 \cdots e_{i-1} e_{i+1} \cdots e_N)}$ to obtain classical RSA signatures $s_i = x^{d_i}$. Note that if m_i denotes the modulus for the public key e_i, then $m_1 \cdots m_N$ will be an appropriate modulus for $r^{e_1 \cdots e_N}$. The individual modulus m_i can then be used by the i-th signer to sign the common blinded data x' and by the recipient of the blind signatures to do the unblinding.

Schnorr Based Threshold Blind Signature

To realize such a scheme based on Schnorr, we can use the threshold blind signature scheme introduced by Jinho Kim et al. [KKL02]. The original scheme describes the following message flow for the message signing procedure:[4]

1. $V \rightarrow A_i: \omega_i = \prod_{k=1, k \neq i}^{t} \frac{k}{k-i}$
2. $A_i \rightarrow V: e_i = g^{t_i} h^{u_i} \bmod p$ where $t, u \in_R Z_q$ and g, h, p setup parameters
3. $V \rightarrow A_i: x' = \varepsilon - \delta$ where $\varepsilon = H(x, \hat{e})$, $\hat{e} = e g^{\beta} h^{\gamma} y^{\delta} \bmod p$, $e = \prod_{i=1}^{t} e_i$ and $\beta, \gamma, \delta \in_R Z_q$
4. $A_i \rightarrow V: (R_i, S_i)$ where $R_i = t_i - x' r_i \omega_i \bmod q$, $S_i = u_i - x' s_i \omega_i \bmod q$ with r_i, s_i public key of A_i.

However, even this protocol is still prone to the attack, if used without public registration board, and hence the message flow has to be adapted[5] in order to gain democracy using this protocol:

1. $A_i \Rightarrow board: (e_i, id_V)$ for each eligible voter
2. $V \Rightarrow board: (\omega_i, x', id_{A_i})$ for at least t authorities
3. $A_i \Rightarrow board: (R_i, S_i, id_V)$

Each authority calculates the commitment for each eligible voter in advance and places them on the public board next to the voter id. Any voter can then start the blinding and signature process. The voter is allowed to present one and only one blinded data x' on the public registration board.

4 Security Analysis

The question whether the attack presented in Section-2 is still possible, can be denied rather intuitively. Every voter can send only one message (a commitment to the voters vote) to be signed to the public registration board. Every registration authority provably

[4] For the sake of readability, the protocol steps presented are stripped down to the signing process. Please refer to the original paper for a more detailed view of the complete protocol.

[5] $\Rightarrow$ indicates that each message has to be signed by the sender.

signs the very same message per voter. Therefore, no threshold attack can be executed any more, and democracy is established under such circumstances.

We now have to prove that the revision does not introduces other security issues for the whole e-voting process.

Anonymity: The introduction of the public registration board seems to raise an anonymity issue. But this is not the case as the only information that can be learned through the public registration board is the fact that some voter initiated the e-voting process. But nothing can be learned of the vote itself nor its containing data. Furthermore, it is not possible to trace the voter's vote. This results in the inability to know if a voter really finished the e-voting process by casting the vote.

Democracy: In the revised protocol the registration authorities do not sign the blinded encrypted vote any more but its blinded hash-value. The consequence of this refinement comes into operation only during the vote casting process. As a blindly signed message is a valid message, the public voting board accepts it as being authorized. As a consequence of this, the voting board could be tainted by receiving signed messages from the public registration board. These votes, however, would be invalid and would not affect the final tally. On the other hand, this is a serious issue, and it can be addressed by letting the voting board to accept only the following tuple: Encrypted vote, and the signatures of the hash-value of the encrypted vote.

Persistence: The use of the public registration board implies the permanent storage of the signatures. Hence, the voter does not need to keep them anymore. The only information the voter needs to keep at a safe place is the blinding factor.

Privacy: If all involved registration authorities collude against a single voter, the voter's privacy is still warranted by the blinding factor the voter has chosen, since finding the correct blinding factor is considered hard [Be01], [KKL02].

5 Conclusion

In this paper we demonstrated that any blind signature protocol with threshold bears an intrinsic weakness on democracy and unforgeability of votes, if no public registration board is in use. The public registration board acts as a point of synchronization, where each voter has to give the commitment to only one single blinded message, ready to be signed by all signing authorities. Therefore, a public board not only serves as a means for individual and universal verifiability. The public registration board is an imperative instrument of communication to multiple authorities within a threshold system. Furthermore, we showed that the special requirement, the provably signing the same data, by multiple signers within the threshold signature scheme based on RSA or on Schnorr can be achieved by a refinement of the blinding/unblinding process.

Bibliography

[AW07] Aeby, A., and M. Wiget. 2007. On-Line Meinungsumfragen. Diploma thesis, Bern University of Applied Sciences. Biel, Switzerland.

[AFT07] Anane, R., R. Freeland, and G. Theodoropoulos. 2007. E-voting requirements and implementation. In *CEC '07, 9th IEEE Conference on E-Commerce Technology*, 382–392. Tokyo, Japan.

[Ba94] Baraani-Dastjerdi, A., J. Pieprzyk, and R. Safavi-Naini. 1994. A practical electronic voting protocol using threshold schemes. Technical report. Wollongon, Australia: University of Wollongong, Department of Computer Science.

[Ba05] Baiardi, F., A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli. 2005. SEAS, a secure e-voting protocol. Design and implementation. *Computers & Security* 24(8): 642–652.

[Be01] Bellare, M., C. Namprempre, D. Pointcheval, and M. Semanko. 2001. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme.

[Bo03] Boldyreva, A. 2003. Threshold signatures, multi-signatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In *PKC'03, 6th international workshop on theory and practice in public key cryptography, LNCS 2567*, ed. Y. Desmedt, 31–46. Miami, FL USA.

[CC96] Cranor, L. F., and R. K. Cytron. 1996. Design and implementation of a practical security-conscious electronic polling system. Technical report WUCS-96-02. St. Louis, MO USA: Washington University.

[CC97] Cranor, L. F., and R. K. Cytron. 1997. Sensus: A security-conscious electronic polling system for the internet. In *HICSS-30, 30th Hawaii international conference on system sciences, volume 03,* 561–570. Maui, HI USA.

[CCM08] Clarkson, M. R., S. Chong, and A. C. Myers. Civitas. 2008. Toward a secure voting system. In *SP'08, 29th IEEE symposium on security and privacy*, 354–368. Oakland, CA USA.

[CF85] Cohen, Josh D., and Michael J. Fischer. 1985. A robust and verifiable cryptographically secure election scheme. In *SFCS '85: Proceedings of the 26th annual symposium on foundations of computer science*, 372–382.Washington, DC USA: IEEE Computer Society.

[Ch82] Chaum, D. 1982. Blind signatures for untraceable payments. In *CRYPTO'82, 2nd international cryptology conference*, 199–203. Santa Barbara, CA USA.

[Ch83] Chaum, D. 1983. Blind signature system. In *CRYPTO'83, 3rd international cryptology conference*, 153–156. Santa Barbara, CA USA.

[Be87] Daniel, J., and Benaloh, C. 1987. Verifiable secret-ballot elections. PhD diss., New Haven, CT, USA.

[Du99] DuRette, B. W. 1999. Multiple administrators for electronic voting. Bachelor thesis, Massachusetts Institute of Technology. Boston, MA USA.

[FOO92] Fujioka, A., T. Okamoto, and K. Ohta. 1992. A practical secret voting scheme for large scale elections. In *ASIACRYPT'92, workshop on the theory and application of cryptographic techniques, LNCS 718*, ed. J. Seberry and Y. Zheng, 244–251. Gold Coast, Australia.

[Ge03] Gennaro, Rosario, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. 2003. Revisiting the distributed key generation for discrete-log based cryptosystems.

[He97] Herschberg, M. A. 1997. Secure electronic voting using the world wide web. Master's thesis, Massachusetts Institute of Technology. Boston, MA USA.

[Hi01] Hirt, M. 2001. Multi-party computation. Efficient protocols, general adversaries, and voting. PhD diss., ETH Zürich. Zürich, Switzerland.

[HL09] Heather, James, and David Lundin. 2003. The append-only web bulletin board. In *Formal aspects in security and trust, LNCS 5491*, ed. Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, 242–256.

[JZF03] Joaquim, R., A. Zuquete, and P. Ferreira. 2003. REVS—a robust electronic voting system. In *IADIS international conference e-society 2003*, 95–103. Lisbon, Portugal.

[Ki02] Kim, K. 2002. Killer application of PKI to Internet voting. In *IWAP'02, 2nd international workshop for Asia public key infrastructures.* Taipei, Taiwan.

[KKL02] Kim, J., K. Kim, and C. Lee. 2002. An efficient and provably secure threshold blind signature. In, *ICISC'01, 4th international conference on information security and cryptology, LNCS 2288*, ed. K. Kim, 318–327. Seoul, South Korea.

[Ok97] Okamoto, T. 1997. Receipt-free electronic voting schemes for large scale elections. In *5th international security protocols workshop, LNCS 1361*, ed. B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, 25–35. Paris, France.

[Oh99] Ohkubo, M., F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. In *ISW'99, 2nd international workshop on information security, LNCS 1729*, ed. M. Mambo and Y. Zheng, 225–234. Kuala Lumpur, Malaysia.

[RRN01] Ray, I., I. Ray, and N. Narasimhamurthi. 2001. An anonymous electronic voting protocol for voting over the internet. In *WECWIS'01, 3rd international workshop on advanced issues of e-commerce and web-based information systems*, 188–191. San Jose, CA USA.

[Sc90] Schnorr, Claus-Peter. 1990. Efficient identification and signatures for smart cards. In *CRYPTO '89: proceedings of the 9th annual international cryptology conference on advances in cryptology*, 239–252. London, UK: Springer-Verlag.

Session 8: Theoretical and Practical Implications of E-Voting

Coercion-Resistant Hybrid Voting Systems[1]

Oliver Spycher[1], Rolf Haenni[2], and Eric Dubuis[2]

[1]Department of Computer Science
University of Fribourg
Boulevard de Pérolles 90
CH-1700 Fribourg, Switzerland
oliver.spycher@unifr.ch

[2]Research Institute for Security in the Information Society
Bern University of Applied Sciences
Quellgasse 21, Postfach
CH-2501 Biel, Switzerland
{rolf.haenni,eric.dubuis}@bfh.ch

Abstract: This paper proposes hybrid voting systems as a solution for the vote buying and voter coercion problem of electronic voting systems. The key idea is to allow voters to revoke and overrule their electronic votes at the polling station. We analyze the potential and pitfalls of such revocation procedures and give concrete recommendations on how to build a hybrid system offering coercion-resistance based on this feature. Our solution may be of interest to governments, which aim at integrating paper-based and electronic voting systems rather than replacing the former by the latter.

[1] Research supported by the Hasler Foundation, project No. 09037.

1 Introduction

In consideration of the complexity and manifold vulnerabilities of today's computers and networks, most governments pursue a cautious strategy in introducing electronic means into processes that are so fundamental to running their democracies. Their reservation is particularly distinctive if the technology involves components that are not under their control. The number of countries experimenting with electronic voting over the Internet is therefore still marginal. Estonia and Switzerland, two of the few pioneering countries in Internet elections and referendums (we shall use the general term *voting*), follow the strategy of slowly increasing the number of electronic votes over the years [CH02]. The idea behind keeping this shift at a slow pace is to limit the risk and consequences of fraud in the early stages of the respective project.[2] In the foreseeable future, traditional and electronic voting systems are therefore expected to live side-by-side for quite some time.

Running two or more different voting systems in parallel requires some care. For example, the possibility must be excluded for voters to cast more than one vote, for instance one in each subsystem. The respective systems in Estonia and Switzerland have their own mechanisms to avoid this. The Swiss Canton and Republic of Geneva, for example, issues a voting card that contains a scratch-off panel with a hidden PIN to access the electronic system [CWS06]. Voters that know their PIN can cast their vote electronically. However, a voter needs to show an untouched scratch-off panel to get access to the ballot box or voting booth at the polling station.

Another problem of running more than one voting system in parallel is the fact that the overall voting system is at most as secure as each of its subsystems. If we consider traditional paper-based systems as almost perfectly secure, the security of the overall voting system is directly determined by the security of its electronic subsystem. Every possible weakness of the electronic system automatically poses a security threat to the overall voting system. If for instance the electronic system issues a receipt to the voters that allows them to prove a coercer or vote-buyer how they voted, the overall voting system is subject to fraud. Indeed, *receipt-freeness* and *coercion-resistance* are two of the most difficult properties to achieve in electronic voting systems [BT94, JCJ05, SKR06].

[2] The legitimacy of such concerns has been demonstrated by the negative e-voting experience of several countries. In the Netherlands, for example, all nationwide e-voting activities were stopped in 2007 after the vulnerability of the deployed voting machines had been exposed in public [Lo08].

In this paper, we introduce the concept of a *hybrid voting system*, which is more than just running a traditional paper-based and an electronic voting system in parallel to form what we would call an *integrated voting system*. The idea is to exploit the properties of the paper-based voting infrastructure to overturn the weaknesses of the electronic system. In particular, we suggest hybrid voting systems as integrated voting systems extended by a *vote revocation* mechanism, which allows voters to overrule their electronic votes by casting an additional paper vote at the polling station. The idea is thus similar to the re-voting feature of the Estonian Internet voting system, in which voters can to cast multiple votes electronically, but such that only the last vote is taken into account [MM06]. The principle and possible benefits of counting only the "last ballot" has first been mentioned in [Sk02]. It is our proposed counter-measure against the vote buying and voter coercion problem, which is difficult to avoid in pure e-voting systems.

To motivate and define our concept of a hybrid voting system, we start in Section 2 with a general discussion of the vote buying and voter coercion problem in electronic voting systems. Then we present our understanding of a hybrid voting system and explain why they offer coercion-resistance. In Section 3, we give concrete recommendations of how to build a hybrid system with the vote revocation feature. To make our analysis as generic as possible, we first develop a classification of different e-voting systems by looking at the properties of the underlying electronic ballot boxes. We will argue that a hybrid system that prevents vote buying and voter coercion can always be constructed, if the enclosed electronic voting system guarantees that each voter can unambiguously identify his vote in the electronic ballot box. In Section 4, we summarize the main conclusions of our analysis and refer to some of the open problems.

2 Hybrid Voting Systems

New voting mechanisms will not find acceptance unless they evidently preserve the security level of traditional paper-based voting. This requirement is inherently difficult to fulfil with e-voting systems and it seems that it is not fulfilled to a satisfactory degree by many of the proposed models or existing systems. Two serious types of fraud that are particularly difficult to prevent and which are largely scalable in electronic systems are *vote buying* and *voter coercion*. In the first part of this section, we describe the challenge of building trustworthy e-voting systems that inherently prevent such types of fraud. Then we show how hybrid voting systems may offer voters a means of voting electronically while keeping the possibilities of such types of fraud as scarce as in traditional paper-based systems.

2.1 Vote Buying and Voter Coercion

Whether or not a system has actually implemented required security features is not necessarily transparent to the voters. If they feel that their votes may not even reach the final tally, they might fully restrain from voting electronically and tend to cast their votes in the traditional way, a means of casting votes still likely to be available in the near future. By doing so, they witness the vote reaching the body of the possibly transparent ballot box. Some countries even allow voters to attend the tallying procedure and thus witness the consideration of their votes in the final outcome. To establish a similar level of voters' trust in e-voting systems, it is imperative to give them access to some information that confirms the correct casting of their votes in a convincing way. This confirmation is meant to provide *individual verifiability*, a precondition to trustworthiness of voting systems. The existence of such a confirmation may thus seem like a feature, but since it will generally also convince any third party that a particular vote was cast, it disallows voters to deceive others about their votes. Such information is thus called a voter's *receipt* [BT94]. Its existence is a violation of the voter's privacy, because it opens the door to the following two types of fraud, in which the adversary gets the voter to vote in a prescribed way [Sk02].

Vote Buying The voter will be rewarded by the *vote buyer* for voting in a particular manner. To receive the reward, the voter may actively co-operate with the vote buyer, e.g. by deviating from the normal voting procedure to construct a receipt.

Voter Coercion The voter is put under pressure or threatened by a *coercer* to vote in a particular manner. Here, the voter may only consent to co-operate with the vote buyer as long as the threat is perceived as real.

Note that both forms of exploiting a voting system are largely scalable in an electronic environment. A vote buyer could simply set up a web site explaining the conditions for making easy money, while a coercer could easily post his threats to thousands of voters. In both cases, the attack is only interesting to potential adversaries as long as voters are able to prove them how they voted. Without a receipt, a corrupted voter could simply lie about the vote cast, i.e., the motivation of an adversary even launching such an attack in the first place is likely to be as low as with paper-based votes.

Clearly, it must be a primary objective to establish an e-voting system that is immune to all sorts of vote-buying and voter-coercion attacks, including those in which the adversary gets the voter to abstain from voting or to vote at random. Systems blessed with that immunity are called *coercion-resistant* [JCJ05, SKR06]. Note that coercion-resistance is stronger than mere *receipt-freeness* [BT94, JV06], which alone does not prevent adversaries from getting voters to abstain from voting. In the literature, there are many suggestions for receipt-free or coercion-resistant systems, but most of them rely on unrealistic technical assumptions such as untappable communication channels [BT94, Ok97, HS00, MBC01, LBD03, SKR06, XS06, MN06, CLW08].

2.2 Hybrid Systems

A hybrid voting system offers every voter the choice between either casting a vote electronically or casting a traditional paper vote at the polling station. The key to undermining the possibility of exploiting the electronic subsystem for the above-mentioned types of fraud is to allow the voters to revoke their electronic votes at the polling station and then to let them cast the vote of personal choice in the traditional way, i.e., inside the (presumably) coercion-free environment of the polling station. Clearly, the revocation mechanism must be designed in a way that an adversary cannot find out which votes have been revoked. In Subsection 3.2, we will propose two different solutions to that problem. Both solutions include three different ballot boxes: the *α-box* for the electronic votes, the *β-box* for the vote revocations, and the *γ-box* for the paper votes. The final outcome Σ of the voting can then be calculated as

$$\Sigma = \alpha - \beta + \gamma,$$

where α, β, and γ denote the individual results of the respective ballot boxes.[3] This model with three ballot boxes is illustrated in Figure 1. Depending on the revocation mechanism, the β-box may contain revocations either in electronic form or on paper. Clearly, each vote in the β-box must reflect the corresponding vote from the α-box.

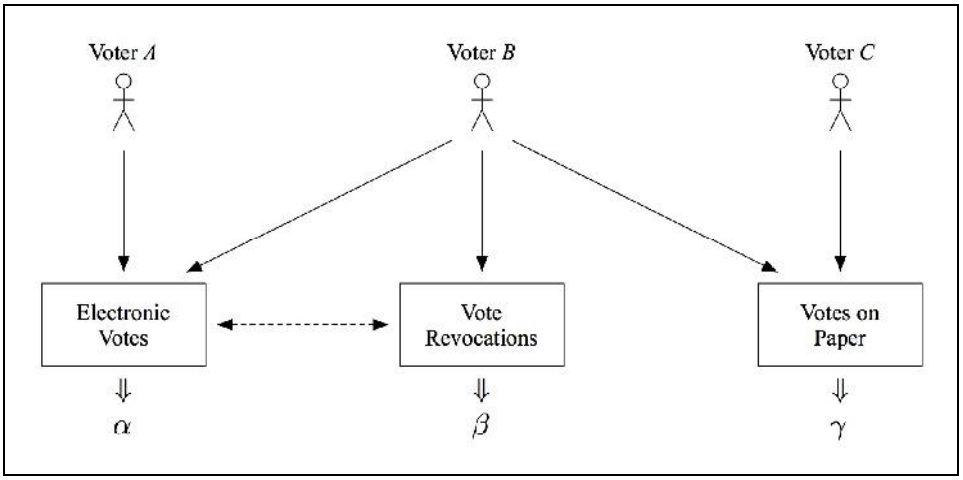


Figure 1: Three types of ballot boxes and voters in a hybrid voting system: Voter *A* votes electronically; Voter *B* first votes electronically, but then overrules it by a paper vote; Voter *C* votes on paper.

[3] We do not further specify here whether the ballot boxes contain simple yes/no-votes or more complicated 1-out-of-*n* or *k*-out-of-*n* selections. In the latter cases, $\Sigma = \alpha - \beta + \gamma$ must be applied component-wise to each of the *n* options.

Coercion-Resistance In a hybrid system with a vote revocation procedure, even if an adversary is contently convinced that the voter cast the electronic vote as told, there is still the possibility that the vote will be overruled by the voter's personal choice and thus not be considered in the final tally. Only by witnessing the voter entering the polling station, it becomes apparent to the coercer that the voter's intention is most likely to revoke the vote. However, monitoring the entrance of a polling station is not easily scalable to a large number of corrupted voters. Furthermore, since the possibility of hindering voters from going to the polling station is also given in traditional, well-accepted paper-based systems, it does not prevent hybrid systems from reaching the same level of coercion-resistance as their traditional counterparts.

We conclude that if adversaries must assume that corrupted voters will usually revoke their votes, a hybrid system is clearly coercion-resistant: an attack would simply seem too expensive. We believe that it is possible for governments to invoke that perception among adversaries, for instance by explicitly allowing voters to cooperate with vote buyers and coercers, however only as long as they revoke their biased vote.

Prerequisites Remarkably, pure electronic voting systems and the electronic subsystems of hybrid voting systems do not necessarily share the same prerequisites. For example, the great challenge of removing receipts from pure e-voting systems does no longer apply to the electronic components of a hybrid voting system. Not only are receipts admitted, their guaranteed presence may even be a prerequisite in the design of a hybrid system. One of the proposed methods in Subsection 3.2 requires such guaranteed receipts. In general, we are less restrictive by imposing the following two basic prerequisites for the e-voting component of a hybrid voting system:

1. The system guarantees the presence of a vote identifier to ensure that the voters can identify the votes in the α-box that were generated using their credentials. Receipts are special cases of such vote identifiers.

2. The system provides some mechanism that allows voting officials at the polling station to check whether or not a registered voter has already cast an electronic vote.

Voting systems complying with the second prerequisite form an integrated voting system. Note that in general the guaranteed existence of a vote identifier (first prerequisite) is insufficient for the voting officials to verify whether someone has cast an electronic vote or not (second prerequisite). Because if such an identifier is secret to the voter, the existence of the electronic vote could be concealed by simply withholding the identifier. Complying with the first prerequisite alone does not therefore imply the property of an integrated voting system. Similarly, the existence of a mechanism to check if somebody has already voted electronically (second prerequisite) is in general not enough to identify that person's vote in the α-box (first prerequisite), because the system may provide a list of voters that is completely disconnected from the list of votes. Thus, hybrid voting systems form a stronger notion than mere integrated voting systems.

In the absence of a receipt, the first prerequisite can be met by leaving the encrypted vote attached to information that publicly identifies the voter. In order to preserve the voters' privacy, the individual votes clearly may never be decrypted in this case, not even at the time of tallying. Instead, homomorphic methods for tallying exist, where only the result of the tally needs to be decrypted [CGS97, HS00]. By applying this method, even the second requirement is inherently met. We thus conclude that the prerequisites we impose on the electronic subsystem of a hybrid system do not form obstacles that are particularly hard to overcome.

3 Vote Revocations in Hybrid Systems

We now consider the construction of a coercion-resistant hybrid voting system. To prevent vote buying and voter coercion, we need to define a secure vote revocation mechanism that allows voters to update their electronic votes at the polling station. For the solution presented in this section, we assume that the electronic subsystem provides the two key prerequisites discussed at the end of the previous section. We assume thus the existence of an electronic ballot box, in which the electronic votes are collected (the α-box). Additionally, we suppose that the traditional voting infrastructure satisfies the following three minimal requirements.

1. The traditional voting infrastructure consists of a polling station, where the paper votes of registered voters are anonymously collected in a physical ballot box (the γ-box).

2. The traditional voting procedure at the polling station (checking the identity of voters, opening the ballot box, counting the votes, etc.) is sufficiently secure, in particular coercion-resistant, and the voting officials are reliable and trustworthy.

3. The official voting period at the polling station chronologically succeeds the electronic voting period.

To understand the applicability of the proposed vote revocation procedures, we first need to get an overview of the different types of electronic ballot boxes in e-voting systems. The result of this discussion in Subsection 3.1 is a classification of e-voting systems, from which two fundamentally different situations emerge. For each of these cases, we propose in Subsection 3.2 a corresponding vote revocation procedure that fits into the proposed counting scheme of a hybrid system.

3.1 Classification of E-Voting Systems

A common core component of all existing e-voting systems is an electronic ballot box, in which votes are collected during the voting period. One can think of it as a database with two basic operations for adding new entries and reading its content. To ensure the availability and the correctness of these operations, and to guarantee the integrity and consistency of the database, a variety of security measures need to be implemented. Some of these measures aim at avoiding so-called single points of failure, i.e., critical components capable of causing the entire system to fail.

Depending on the chosen configuration and properties of the electronic ballot box and the structure of its entries, different e-voting systems emerge. In the remainder of this subsection, we will make a distinction between black box and bulletin board systems, anonymous and non-anonymous boards, identifiable and non-identifiable board entries, and the presence or absence of a receipt. In Figure 2, we give a first overview of this classification and indicate where vote revocations are possible.

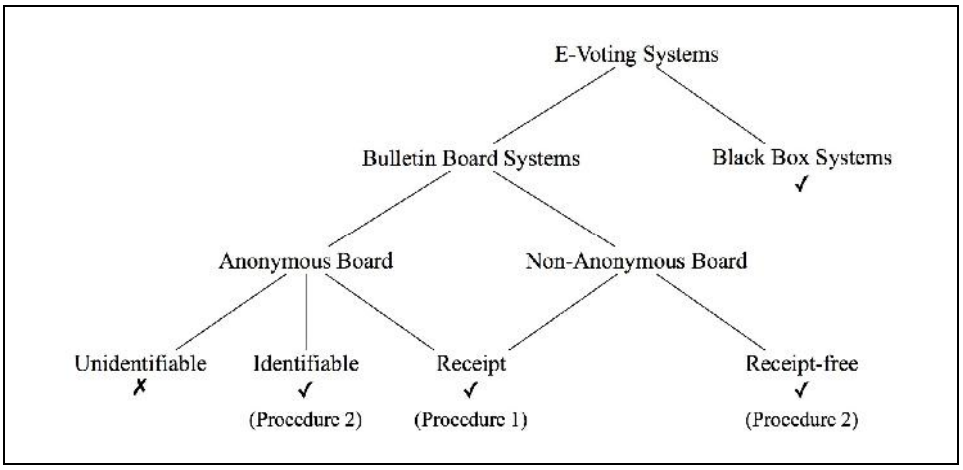


Figure 2: Classification of existing e-voting systems with different types of electronic ballot boxes. The check marks indicate where vote revocations are possible.

Black Box vs. Bulletin Board Systems E-voting systems mainly differ in the type of database access they provide. There are two extreme cases, one in which the access is restricted to a few authorized persons only and one in which everybody can add new entries to the database and read its contents (while deleting entries is always prohibited). E-voting systems of the first category are sometimes called black box voting systems [HA03, KKW06]. They are very popular in commercial solutions and in existing political e-voting projects. An advantage of black box systems is that from a cryptographic point of view, they are relatively simple to understand and implement. On the other hand, they are often criticized as not providing enough transparency, i.e., neither providing individual verifiability nor allowing the outcome to be publicly verified.

The second major category comprises systems with a public bulletin board, through which all cast votes are visible to everybody [Pe05]. To ensure the secrecy of the votes and the fairness of the voting process, the board's entries need to be encrypted (at least during the official voting period). The purpose of the public board is to allow all voters to verify the inclusion of their votes in the electronic ballot box and the correctness of the counting. Most system proposals in the scientific e-voting literature are based on such bulletin boards.

Anonymous vs. Non-Anonymous Boards In bulletin board systems, there are two opposed subcategories, each defined by whether the entries on the board are anonymous or not. In the case of anonymous boards, there must be an additional mechanism to exclude votes from unauthorized voters or multiple votes from the same voter. Examples of such mechanisms are mix nets [Ch81] or blind signatures [Ch82]. If the board entries are not anonymous, for example if they contain a unique voter ID that attributes them unambiguously to the respective voters, there must be a mechanism that prevents the decryption of single votes. Systems of that type are usually based on homomorphic encryption schemes with a shared public key [CGS97, HS00]. Clearly, in those systems, the publicly known voter ID serves as the vote identifier.

Vote Identifiers vs. Receipts Another distinguishing feature of bulletin board systems concerns the board entries themselves. There are three basic types: those which can be identified and disclosed with a receipt, those which can only be identified with a vote identifier (but not disclosed), and those which are completely unidentifiable. In the case of a non-anonymous board, where the identification of the votes is given intrinsically, only two types of board entries remain, those with a receipt and those without. These cases are depicted at the bottom of the tree shown in Figure 2.

3.2 Vote Revocation

In the classification tree of the previous subsection, four cases are tagged with a check mark and one is crossed out. The cross means that the case of an anonymous board with unidentifiable board entries is not compatible with any vote revocation procedure. The missing vote identifier makes it impossible to either remove the vote from the electronic ballot box or to subtract it from the final tally. Note that by explicitly requiring the existence of vote identifiers at the end of Section 3, we had already ruled out this case from the beginning.

In black box systems, it is possible to install a vote revocation mechanism as long as the electronic votes in the ballot box remain identifiable. Due to the lack of transparency offered by such systems, the correct application of a potential revocation mechanism cannot be verified by the public. We therefore leave revocations using a black box approach undiscussed.

Procedure 1: Revocations on Paper The first procedure we propose assumes that every voter owns a receipt for his vote in the α-box. It does not matter whether the board is anonymous or not, but it is crucial that the voter (and not the coercer or vote buyer alone) is in possession of the receipt. The payoff of this restriction is a revocation procedure that is particularly appealing in its simplicity.

The following points define the procedure. We start off when the voter at the polling station is about to revoke the electronic vote in the α-box, i.e., we assume that the voting officials have already successfully checked the voter's identity and right to vote.

1. The voter uses the receipt to locate the encrypted vote in the α-box and reveal it to the voting officials.

2. The voting officials prepare a revocation paper ballot containing the same vote and hand it over to the voter.

3. The voting officials verify that the voter drops the revocation paper ballot into the β-box.

4. The voter is granted access to the γ-box to cast the final paper vote.

In this procedure, the β-box is thus a physical ballot box similar to the γ-box. At the end of the official voting period, it is opened and tallied according to the same tallying procedure.

In the scheme as it is proposed, it is crucial to assume that the voting officials will not allow the voters to cast a paper ballot that differs from their electronic votes in the α-box. If not all voting officials are fully trustworthy, then several voting officials should be involved in each step of the procedure. In other words, before the voter gets access to the γ-box, a sufficient number of voting officials would have to give their approval, for instance by signing the revocation ballot. Thus, we merely need to assume that among the group of involved voting officials, there is at least one that would refuse the signature to an incorrect revocation ballot.

A drawback of this procedure is the fact that the content of the electronic vote must be revealed to the voting officials. One could argue that this violates the anonymity of the vote, because in a simple yes/no-type of voting, evoking a yes-vote implies that the update will be a no-vote, and vice versa. But since such conclusions will always remain speculative, i.e., it cannot be excluded that the original and the updated votes are identical, we think that this is an unpleasant, but acceptable side effect.

Note that by requiring instead of avoiding a receipt, we sharply depart from the mainstream approach of taking additional measures to make electronic voting systems receipt-free. Yet, the following procedure shows how vote revocations can be realized even without receipts.

Procedure 2: Electronic Revocations Let the e-voting component of the hybrid system now be a system that provides a mere vote identifier, not necessarily a receipt. The idea then is to leave the votes encrypted throughout the whole revocation procedure. To guarantee the anonymity of those who decide to revoke their votes, and thus to ensure the overall system remains coercion-resistant, we define the β-box as an anonymous bulletin board to which re-encryptions of the original votes are posted. The adversary is then unable to make out which votes from the α-box have been revoked. The electronic voting environment must therefore comply with the following additional requirements.

- The β-box must be an anonymous bulletin board.
- The encryption scheme used to generate the encrypted votes in the α-box must allow re-encryption[4] and the generation of non-transferable proofs of correct re-encryption.[5]

[4] Let $w = E(v, r)$ be the encrypted vote, where E is a randomized encryption function with randomization factor r. Then $w' = R(w,r')$ denotes the re-encryption of w, such that the decryptions of w and w' are identical, i.e., $v = D(w) = D(w')$.

[5] A proof of correct re-encryption allows a prover to convince a verifier that w' is indeed a re-encryption $R(w,r')$ of w, without revealing the randomization factor r'. A proof constructed as an *interactive* Σ*-protocol* is inherently non-transferable, i.e., only the involved verifier will be convinced of its correctness [BG92]. Corresponding non-interactive protocols are transferable, but there is a general way of extending them to be convincing to a designated verifier only [JSI96].

The following steps define the proposed procedure:

1. The voter generates a re-encryption of the encrypted vote in the α-box.
2. A corresponding non-transferable proof of correct re-encryption is generated, designated to the voting officials at the polling station. Optionally, this step can be done remotely in a non-interactive manner.
3. The voter approaches the voting officials and uses the vote identifier to identify the encrypted vote in the α-box.
4. The voter hands the re-encryption and the corresponding non-transferable proof over to the voting officials.
5. If the delivered proof is valid, the voting officials post the re-encrypted vote to the β-box.
6. The voter is granted access to the γ-box to cast the final paper vote.

The electronic β-box is tallied according to the tallying procedure defined for the α-box.

Similarly to Procedure 1, we can enhance the scheme by requiring a sufficient number of voting officials to approve the correctness of the voter's re-encryption, i.e., a voter would only be granted access to the γ-box if sufficiently many voting officials have posted their electronic signatures of the re-encryption to the bulletin board.

Clearly, the randomization factor used for the re-encryption may serve as a receipt. The voter can therefore always prove to an adversary that the electronic vote has been revoked, but he or she will never be interested in doing so. On the other hand, the receipt does not help to prove to an adversary that the electronic vote has *not* been revoked. It thus does not reduce the security level of the overall system.

4 Conclusion

Governments around the world intend to offer their citizens e-voting as a comfortable way to express their political preferences. Yet, it seems that the traditional paper-based schemes are not likely to disappear for some decades. Defining procedures that integrate both means of casting votes to an overall voting system clearly poses an inherent necessity. We propose our understanding of hybrid voting systems as a solution to this challenge. By introducing the anonymous β-box and by exploiting the traditional polling station as a protective environment, we allow voters to revoke their electronically casted votes. We argue why such an approach yields coercion-resistance, even if the electronic subsystem were indeed subject to coercion. In a hybrid system, we are therefore given the freedom to have an e-voting subsystem that grants receipts to satisfy individual verifiability, without introducing the risk of vote buying or voter coercion.

Bibliography

[BG92] M. Bellare and O. Goldreich. On defining proofs of knowledge. In E. F. Brickell, editor, CRYPTO'92, 12th Annual International Cryptology Conference on Advances in Cryptology, LNCS 740, pages 390– 420, Santa Barbara, USA, 1992.

[BT94] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In STOC'94, 26th Annual ACM Symposium on Theory of Computing, pages 544–553, Montréal, Canada, 1994.

[CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications, 8(5):481–490, 1997.

[Ch81] D. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. Communications of the ACM, 24(2):84–88, 1981.

[Ch82] D. Chaum. Blind signatures for untraceable payments. In CRYPTO'82, 2nd International Cryptology Conference, pages 199– 203, Santa Barbara, USA, 1982.

[CLW08] S. S. M. Chow, J. K. Liu, and D. S. Wong. Robust receipt-free election system with ballot secrecy and verifiability. In NDSS'08, 15th Network and Distributed System Security Symposium, pages 81– 94, San Diego, USA, 2008.

[CWS06] M. Chevallier, M. Warynski, and A. Sandoz. Success factors of Geneva's e-voting system. Electronic Journal of e-Government, 4(2), 2006.

[Di02] Die Bundesbehörden der Schweizerischen Eidgenossenschaft. Bericht über den Vote Electronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte. Bundesblatt, 154(5):645–700, 2002.

[DKR06] S. Delaune, S. Kremer, and M. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In CSFW'06: 19th IEEE workshop on Computer Security Foundations, pages 28–42, Venice, Italy, 2006.

[HA03] B. Harris and D. Allen. Black Box Voting: Ballot Tampering in the 21st Century. Plan Nine Publishing, 2003.

[HS00] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, EUROCRYPT'00, International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 1807, pages 539–556, Bruges, Belgium, 2000.

[JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In V. Atluri, S. De Capitani di Vimercati, and R. Dingledine, editors, WPES'05, 4th ACM Workshop on Privacy in the Electronic Society, pages 61–70, Alexandria, USA, 2005.

[JSI96] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In U. Maurer, editor, EUROCRYPT'96, International Conference on the Theory and Application of Cryptographic Techniques, LNCS 1070, pages 143–154, Saragossa, Spain, 1996.

[JV06] H. L. Jonker and E. P. Vink. Formalizing receipt-freeness. In ISC'06, 9th Information Security Conference, LNCS 4176, pages 476–488, Samos, Greece, 2006.

[KKW06] A. Kiayias, M. Korman, and D. Walluck. An internet voting system supporting user privacy. In ACSAC'06, 22nd Annual Computer Security Applications Conference, pages 165–174, Miami Beach, USA, 2006.

[LBD03] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, ICISC'03, 6th International Conference on Information Security and Cryptology, LNCS 2971, pages 245–258, Seoul, Korea, 2003.

[Lo08] L. Loeber. E-voting in the Netherlands: from general acceptance to general doubt in two years. In R. Krimmer and R. Grimm, editors, 3nd International Workshop on Electronic Voting, Lecture Notes in Informatics, pages 21–30, Bregenz, Austria, 2008. Gesellschaft für Informatik E.V.

[MBC01] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In B. Schmid, K. Stanoevska-Slabeva, and V. Tschammer, editors, I3E'01, 1st IFIP Conference on towards the E-Society, volume 202, pages 683–694, 2001.

[MM06] Ü. Madise and T. Martens. E-voting in Estonia 2005: The first practice of country-wide binding internet voting in the world. In R. Krimmer, editor, 2nd International Workshop on Electronic Voting, number P-86 in Lecture Notes in Informatics, pages 15–26, Bregenz, Austria, 2006. Gesellschaft für Informatik E.V.

[MN06] T. Moran and M. Naor. Receipt-free universally-verifiable voting with everlasting privacy. In C. Dwork, editor, CRYPTO'06, 26th Annual International Cryptology Conference on Advances in Cryptology, LNCS 4117, pages 373–392, Santa Barbara, USA, 2006.

[Ok97] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, editors, 5th International Security Protocols Workshop, LNCS 1361, pages 25–35, Paris, France, 1997.

[Pe05] R. A. Peters. A secure bulletin board. Master's thesis, Department of Mathematics and Computing Science, Technische Universiteit Eindhoven, The Netherlands, 2005.

[Sk02] J. Skripsky. Minimal models for receipt-free voting. Semester project, ETH Zürich, 2002.

[XS06] Z. Xia and S. Schneider. A new receipt-free e-voting scheme based on blind signature. In WOTE'06, IAVoSS Workshop on Trustworthy Elections, pages 127–135, Cambridge, U.K., 2006.

E-voting in Japan: A developing case?

Masahiro Iwasaki

College of Law
Nihon University
2-3-1 Misaki-cho, Chiyoda-ku,
Tokyo 101-8375
JAPAN
iwasaki@mtj.biglobe.ne.jp

Abstract: This paper aims to introduce the current situation of electronic voting (e-voting) in Japan and discuss its challenges. E-voting has gradually spread in Japan. It has been used a total of twenty times by ten local governments since it was first introduced in 2002. Under the current law, e-voting can be used only for the election of the head of local government or council members. The paper first introduces the actual state of e-voting in Japan. Then the current status and challenges of the electronic voting system are analyzed based on data obtained from the experiences of Japanese cases. Finally, the paper discusses what challenges the Japanese e-voting has, and what could be given as prescriptions for them.

1 Current Status of E-voting in Japan

In 2002, the first electronic voting (e-voting) was realized in Japan. Since then, ten local governments conducted a total of twenty cases of e-voting. In Japan, after "e-Japan Strategy[1]," which aims to build an electronic government (e-government[2]), was published in January 2001 many efforts toward an electronic government (e-democracy) and electronic democracy have been attempted[3]. E-voting can be considered within this trend[4].

This paper aims to introduce the current status of e-voting in Japan and to discuss its challenges. The paper first introduces the actual state of e-voting in Japan. Then the current status and challenges of the electronic voting system are analyzed based on data obtained from experiences of Japanese cases[5]. Finally, the paper discusses what challenges Japanese e-voting has, and what could be given as prescriptions for them.
In Japan, the "Act on Special Provisions Concerning Voting Method by Means of

[1] http://www.kantei.go.jp/jp/singi/it2/kettei/010122honbun.html
[2] See [An07], [Ha99], [Ho08], [Kh09], and [No01].
[3] The concept of "electronic democracy" is vague and it has various meanings. See [Fe00], [Gi04, [Ha99], [Hi98], [Iw05], [To98], and [Ts98].
[4] http://www.kantei.go.jp/jp/singi/it2/index.html
[5] See [Iw04] and [Iw09].

Electromagnetic Recording Voting Devices Used for Election of Council Members and Heads of Local Governments (hereafter 'E-voting Act')" was enacted in the 153rd extraordinary Diet session on November 30, 2001[6]. The Act was issued on 7 December and put into effect on 1 February 2002, which enabled e-voting for local elections. The E-voting Act is intended only for elections of a local government head or a member of a local council. Each local government is required to establish its own ordinance before holding any e-voting.

For example, in the case of Niimi City, Okayama Prefecture, Niimi City Council enacted the "Ordinance Concerning Voting by Means of Electromagnetic Recording Voting Devices Used for Elections of Council Members and Mayor of Niimi City" in March 2002[7]. This enabled e-voting in the double election of Niimi City Mayor and the Council members on 23 June of the same year[8]. Since then, there have been total of twenty cases of e-voting by ten local governments[9]. This number indicates that the dawn of e-voting in Japan is over and the country is now in the phase of establishment.

2 Introductory Phase of E-voting

According to the E-voting Act, e-voting is defined as a means of voting that uses a device. The current procedures for such an electronic voting method in Japan are as follows:

- First, an elector goes to a designated polling station on an election day.
- The elector is required to bring an admission ticket to his/her polling station, which s/he has received in the mail in advance.
- When the elector hands the admission ticket to the reception at the polling station, a staff person checks his/her identification by comparing the name of the elector with the register of electors.
- When the personal identification has been confirmed, a voting card is issued from a voting card issuing device by the staff, which is handed to the elector.
- The elector stands in front of a voting device and inserts the voting card; this initiates the device.

[6] http://www.soumu.go.jp/senkyo/senkyo_s/news/touhyou/denjiteki/pdf/houritsu.pdf

[7] We can experience a demonstration of e-voting on the website of Niimi City. http://www.city.niimi.okayama.jp/?ID=10973

[8] http://www.city.niimi.okayama.jp/?ID=9901

[9] A total of twenty cases of e-voting by ten local governments are as follows: (1) Niimi City, Okayama Prefecture, (2) Hiroshima City, Hiroshima Prefecture, (3) Shiroishi City, Miyagi Prefecture, (4) Sabae City, Fukui Prefecture, (5) Kani City, Gifu Prefecture, (6) Otama Village, Fukushima Prefecture, (7) Ebina City, Kanagawa Prefecture, (8) Rokunohe Town, Aomori Prefecture, (9) Kyoto City, Kyoto, Prefecture, and (10) Yokkaichi City, Mie Prefecture.

・The elector selects a candidate of his/her choice from a list of candidates shown on the touch-panel screen by touching the appropriate name, using his/her finger or a touch pen (if not voting for any candidate, the elector touches a display that says, “Complete without Voting;” this will allow the elector to complete his/her vote without choosing any candidate).
・The elector confirms the selected candidate.
・The voting result is recorded in an electromagnetic recording medium inside the electronic voting device.
・The elector removes the voting card from the voting device.
・The voting process is now complete; the elector returns the voting card at the exit, and leaves the polling station.

Contrary, the current procedures for a traditional paper ballot voting method in Japan (which is called “self-write voting”) are as follows:

・First, an elector goes to a designated polling station on an election day.
・The elector is required to bring an admission ticket to his/her polling station, which s/he has received in the mail in advance.
・When the elector hands the admission ticket to the reception at the polling station, a staff person checks his/her identification by comparing the name of the elector with the register of electors.
・When the personal identification has been confirmed, a ballot paper is handed to the elector by the staff.
・The elector writes the name of a candidate from a list of candidates (if not voting for any candidate, the elector does not write any name; this will allow the elector to complete his/her vote without choosing any candidate).
・The elector casts the ballot paper into the ballot box.
・The voting process is now complete; the elector leaves the polling station.

Therefore, e-voting in Japan is considered an evolved form of self-write voting, rather than a method completely different from the conventional self-write voting. The Study Group describes this aspect in detail in a report on “Election Systems Using Electronic Devices within the Ministry of Internal Affairs and Communications[10].”

[10] http://www.soumu.go.jp/menu_news/s-news/2002/pdf/020201_2.pdf

On 30 July 1999, the former Ministry of Home Affairs established the Study Group on Election Systems Using Electronic Devices. The Group released the final report on 1 February 2002, indicating that the introduction of e-voting has three phases as described below. In Japan, the implementation of the first phase has been the focus.

- The first phase is when an elector votes using an electronic voting device at a designated polling station.
- The second phase is when an elector can vote at a polling station other than a designated one.
- The third phase is when voting at a polling station is not required, and an elector votes using a privately-owned computer terminal.

The first phase is the form that has been implemented in Japan. In this phase, electronic voting devices are not connected to any network; they are individually installed both in polling stations and vote-counting stations. An elector has to go to a designated polling station as one has always done.

The only difference from the conventional method is that an elector votes by using a voting device, not self-write voting, at a polling station.

When counting votes, the challenge is to find a method to deliver voting data to a vote-counting station. The recording medium that stores voting data is removed from the voting device at the polling station, and delivered to the vote-counting site. This is the same procedure as the one in self-write voting, where the ballot box holding ballot paper is delivered to the vote-counting station.

Currently, the recording medium that stores data is hand-delivered from the polling station to the vote-counting station by election staff. The other possible delivery method is to send the data over a network connecting the polling station and vote-counting site. This method has not been adopted in the first phase since it still contains various issues, including security.

The second phase networks includes voting devices installed at polling stations with a dedicated line. The line used in this phase is to be closed for security issues. The register of electors needs to be networked for the personal identification of electors at polling stations. The network is also necessary to share information about the candidates.

In the second phase, voting at a polling station other than a current designated one becomes possible. In this case, either of the following will be chosen: (1) voting at any polling station within the same electoral district; (2) voting at any polling station within all the electoral districts of the same election; and (3) voting at any site including areas not having an election.

The voting at any polling station within the same electoral district enables an elector to vote at a nearby polling station in an area where s/he lives, rather than a current designated polling station. For example, an elector can vote at the closest polling station when s/he goes out for shopping.

The voting at any polling station within all the electoral districts of the same election enables, for example, an elector to vote at any polling station within a prefecture, if it is for a prefectural election. For the election of Tokyo Metropolitan Mayor, an elector can vote in any ward other than Chiyoda Ward even if it is not his/her designated polling station.

The voting at any site including areas not having an election enables an elector to vote in Kyoto Prefecture, if there is a polling station, even when the election is for Tokyo Metropolitan. Also, an elector can vote at a site other than a polling station if it is authorized for voting.

For all of the above three scenarios in the second phase, establishing a network for the register of electors or for sharing candidate information will be necessary. The register of electors is used for identifying if a person who comes to vote is a particular elector, and the list will be operable depending on the status of the Basic Resident Registers Network and Local Government Wide Area Network.

In the third phase, instead of requiring electors to vote at polling stations as a conventional system does, it is assumed that a computer owned by each elector would be used for voting. If all elections are conducted by the third phase method, a polling station itself may become unnecessary. In this phase, a standard internet connection, not a dedicated line, would be utilized as each individual's computer is used. Thus security issues are unavoidable. Also, the issue of the Digital Divide–including whether an elector can use a computer and whether s/he has a computer, or not–becomes crucial.

The problem of identification at the time of voting also emerges. Since identification based on a register of electors at a polling station is not performed in the third phase, as the current system does, it is difficult to identify if a person sitting in front of a computer is a particular elector. Therefore, it is necessary to prevent impersonation by identity verification with public key cryptography as well as biometrics using fingerprints and irises.

In addition, since third parties such as observers at a polling station do not exist in the third phase, it becomes unclear if a voting individual is voting based on his/her true free will. For example, there could be a possibility that an elector is forced to vote for a particular candidate under abduction/confinement. Considering that the existence of observers at polling stations in the current system guaranties the transparency of elections, it is crucial how to resolve the transparency issue in the third phase voting.

Judging from the evolution of ICT, it could be possible to implement the third phase e-voting. However, from the perspective of operating an election, the third phase is quite unrealistic. E-voting is still in the first phase in Japan, and it seems more likely that the situation will continue as it is now. There are many issues to be resolved in order to shift to the second phase, and those issues are not easy to solve. It is crucial to steadily accumulate the experiences of e-voting in the first phase[11].

[11] Cf. [Ke04].

3 Characteristics of E-voting in Japan

The intrinsic changes are overlooked if e-voting is viewed as a mere change from self-write voting to a method using devices. In fact, if one focuses only on e-voting, one's perspective would be that it is just a change of voting methods. However, e-voting indicates a new form of election in an ICT-prevailing society[12]. The newness of e-voting can be described by four aspects: voting, tallying, communication and vote-counting methods.

	Self-write voting	E-voting
Voting method	Using a ballot paper	Using a voting device
Tallying method	Using a ballot box	Using a voting device
Method of communicating voting data	Delivery of the ballot box from the polling station to the vote-counting station	Delivery of the recording medium from the polling station to the vote-counting station
Vote-counting method	Staff	Computer

Table 1: Self-write voting and e-voting in contemporary Japan

First, the voting method differs significantly from conventional self-write voting in using a voting device, and the newness lies in voting with a device instead of voting by a paper ballot. A voter casts a ballot by operating a voting device at a polling station, and the vote is stored as it is in the device. Containing a recording medium that stores voting data, the device plays the double role of writing down the vote onto a paper ballot and accumulating ballots in a ballot box, as it was done in self-write voting. That is in e-voting, the device itself has the double function of casting ballots and storing voting data. This brings both advantages and disadvantages.

The advantages include the simplification of voting for voters due to the use of a device. As the currently-used voting device adopts a touch-panel, the act of voting is done with only a light touch on a screen. For example, it is easier for physically challenged voters to touch a device than self-write voting. It is clear that e-voting makes voting simpler than self-write voting does.

The second advantage is the accuracy of voting, which is related to the first advantage. In e-voting, as a voter chooses a candidate to vote from a list of candidates displayed on

[12] Cf. [Fe00], [Gi03], [Gi04], [Ha00], [Ha99], and [Oa06].

a screen, s/he can only vote for those on the list. However, in self-write voting, voters often write a name other than that of a candidate, or misspell a name, which results in invalid ballots. Voters may also write down only the last name or the first name. In self-write voting, a typical problem is when there are more than one candidate with the same last name; in such a case, votes are equally divided among both candidates. On the contrary, e-voting ensures the accuracy of voting by avoiding the above issue since a voter has no choice, but to vote for candidates displayed on a screen for a certain election.

The third advantage is that of being barrier-free. E-voting leads to a barrier-free system by making it easy for the elderly and the physically-challenged to vote. There are voters who have difficulty writing on ballots with a pencil, and it is easy for them to vote using a device. For those who are optically challenged, voting with audio guidance becomes available by using an appropriate voting device. Such voters can vote at their own pace since they operate the device by listening to audio guidance with headphones and can adjust audio speed. Such voting devices have already been developed in Japan. Although the current voting device supports optical challenges, promoting a barrier-free device for those who are both optically and aurally challenged, or those who are intellectually challenged is an issue to be resolved.

The disadvantages include the failure of a voting device, errors in device operation, and distrust in a voting device such as the leakage of privacy, and the cost issue of a device. In other words, issues related to a device become the disadvantages. If a device fails, voting itself becomes impossible. While bringing many advantages by using a device, e-voting could cause disadvantages exactly because it uses a device.

In fact, there were several cases where voting discontinued due to the failure of a voting device or a device failed due to errors in operation. In the case of Kani City, Gifu Prefecture, the election itself became invalid as it was determined that the failure of their voting devices affected the result.

The possibility of privacy leakage can be noted in terms of distrust of a device. Voters often have a variety of distrust such as: A device might record who voted for whom upon voting; or it is unclear if a ballot was truly cast for the candidate whom the voter has chosen. There is no other solution to clear up as much distrust as possible other than to improve the reliability of e-voting. It can be time consuming; however, it is indispensable to make efforts in establishing reliability.

Additionally, there is the issue that the cost of a voting device is high. Indeed, the E-voting Ordinance was abolished in Sabae City, Fukui Prefecture, due to the high cost[13]. However, a special local grant tax measure is applied when implementing e-voting, and financial support is available according to the number and size of polling and vote-counting stations. More specifically, the amount provided is based on a calculation that multiplies designated unit price depending on the number of polling and vote-counting stations. The special local grant tax amount is the sum of polling station expenses and vote-counting station expenses.

[13] See [Iw04].

Although there exists an image that e-voting is costly, assistance is actually available. It is necessary to provide information about the actual operational status, including the fact that the previous cases adopted rental devices instead of purchased ones. It is not necessarily reality that it takes a tremendous cost and high risks in order to introduce e-voting from scratch.

Next, a tallying method is related to one that stores voting data in an electronic voting device. So far, there are two data recording methods for electronic voting devices: a standalone method and a client-server method. Most of the cases in Japan have adopted the standalone method, although there were two cases that used the client-server method. The two differ in the tallying methods of electronic voting devices. In simple terms, the standalone method is equipped with one recording medium per voting device, while the client-server method uses one recording medium per polling station. In the case of the standalone method, if there are five electronic voting devices at one voting station, five recording media will be delivered from the polling station to the vote-counting station, since each device has one recording medium. The client-server method uses one recording medium per polling station. Thus there is one recording medium however many voting devices are installed at one polling station. One server is set up for each polling station, connecting multiple voting devices, and voting data is collected in the server. In delivering data from the polling station to a vote-counting station, the collected data on the server is transferred to a magneto-optic disk (MO), which will be delivered to the vote-counting station.

Although the two collection methods have their own advantages and disadvantages, there is a reason that the standalone method is more likely to be adopted when considering issues in reality. This method can minimize any damage in case trouble occurs. Even if one voting device fails in a polling station, it can be immediately replaced with a back-up device. In this way, there will be almost no influence on voting that follows. As the recording medium equipped in the failed machine has the voting data up to the time of the failure, it is delivered to the vote-counting station. Obviously, the voting data reflects the will of voters, thus it cannot be made invalid or destroyed. The standalone method provides two recording media; one is original and the other is a duplicate. Therefore, if the original recording medium did not store data properly, or the medium was damaged, the duplicate can serve in place of the original.

On the other hand, since the client-server method collects voting data in one recording medium by a server regardless of the number of voting devices at a polling station, there is a possibility that all of the voting devices at the polling station would be unusable if the server fails. Even if each voting device is operable, voting is no longer possible as voting data cannot be recorded. In fact, trouble due to server failure occurred in the e-voting in Kani City in July 2003. Later, a lawsuit was initiated regarding the e-voting in Kani City, and the election itself was determined invalid.

Based on such history, the standalone method is more widely adopted[14]. The collection method for e-voting employs a voting device that stores voting data in a recording medium, which leads to a question: An indication that paper medium should also be used

[14] Exceptionally, two of twenty cases of e-voting in Japan adopted a client-server method. Otama Village and Ebina City used it.

since recording voting data only in a voting device would cause difficulty if the device or its recording medium fail. This is the notion that self-write voting be applied, for use in an emergency, along with e-voting. It is true that this would prevent the loss of voting data at the time of any trouble.

Also, there is a proposal for countermeasures suggesting that paper ballots be prepared in case of device failure and that self-write voting using the paper ballots replace e-voting, if there is any device failure. This proposal would result in higher costs since costs for providing voting devices and preparing paper ballots are both necessary for one election. This leads to a discussion about whether e-voting should be introduced with such costs.

At this moment, there are two methods for tallying, and no alternative method has been proposed or considered to be put into practice. It is worth examining the various methods. However, voting methods or tallying methods that are significantly different from the implementation of e-voting would never facilitate any discussion, even if they were proposed.

Next, methods of communicating voting data are discussed. They are the delivery methods from a polling station to a vote-counting station. What is necessary, when voting time on an election day is over and a polling station is closed, is the delivery of voting data to the vote-counting station. In the case of self-write voting, ballot boxes are delivered to vote-counting stations as they are. In e-voting, a recording medium is removed from the e-voting device, sealed, stored, and locked in a strong container, and delivered to a vote-counting station. Basically the delivery of voting data from a polling station to a vote-counting station is the same as the conventional method. The only difference is whether it is a ballot box with paper ballots inside or a recording medium storing voting data.

At this moment, the delivery of voting data is handled in the same way as the conventional method, since the implementation of e-voting is still in the first phase as it is defined in the report issued by the Ministry of Internal Affairs and Communications' Study Group of Election Systems Using Electronic Devices[15]. When voting time is over, a ballot box is closed and delivered to a vote-counting station by car. Thus the most important factor in e-voting is to deliver a recording medium quickly and safely to a vote-counting station. When e-voting is implemented in the second and third phases in the future, it is unnecessary to maintain the current delivery method. For example, in the second phase, each polling station would have a dedicated network. If security issues such as intrusion by hackers are resolved, voting data can be delivered to a vote-counting station through such network. Then the communication method of voting data will see a dramatic change. In the third phase, voting would be done from a work place or a computer at home. There will be security issues, but it will be significantly different from the current first phase in terms of data delivery. In this phase, further study is needed to determine whether polling stations should be set up, and whether a means of collecting voting data from all voters and delivery it to polling stations is necessary. Also, it is possible to collect all the voting data at each polling station and send them to a vote-counting station, or to send the data accordingly to a vote-counting station through a network.

[15] http://www.soumu.go.jp/menu_news/s-news/2002/pdf/020201_2.pdf

If the second and third phases are implemented, the method of communicating voting data could be transformed significantly while maximizing the advantages of ICT. Although there are mountains of issues to resolve before that, there are various possibilities for future communication methods. Since the current e-voting follows the same conventional method, the advantage of e-voting is not yet very clear in terms of its communication method. In other words, there will be more advantages depending on how communication methods are utilized in e-voting.

The fourth notable point is the vote-counting method. In e-voting, the important task is to read a recording medium delivered to a vote-counting station by a computer, not to take out paper ballots from a ballot box. The reading itself is the vote-counting process. In the standalone method, the more voters an area has, the more recording media there will be, since one electronic voting device has one recording medium. Those who are in charge of vote-counting process would be one staff person who operates the recording media on a computer, and the other who checks and confirms the computer operation, which means that only two people are necessary. Compared to self-write voting, this is a significant cutback in labor, and leads to the reduction of labor costs. When a recording medium is read by a computer, the data is quickly calculated and the voting result is displayed on the screen. The vote-counting result is revealed when the displayed result is printed.

The E-voting Act defines that an electronic voting device shall not be connected to an electric communication line. Thus, this is the limit to reducing vote-counting time. It is because the data must be delivered from the polling station to the vote-counting station, and the current method cannot shorten this delivery time. In the future, if a polling station and a vote-counting station are networked and the delivery of voting data is done in a second over the network, even further reduction of time will be possible. The reasons for prohibiting the connection to electric communication circuits include security issues. Since there is the possibility of unauthorized access from outside, such as by hackers, security measures must be thorough. One option for security measures is use a closed, dedicated network. By doing so, it is possible to prevent unauthorized access.

The advantages of vote-counting methods in the current first phase are as follows: There are no illegible ballots there is no equal division of ballots; there is a reduction of vote-counting time; and a reduction of labor in vote-counting tasks. All of these are significantly different from the conventional self-write voting. The voting, tallying, communication, and vote-counting methods of e-voting have completely different features from those in the conventional self-write voting, thus could achieve significant effect depending on how they are used[16].

[16] See [Iw04] and [Iw09].

4 Issues in E-voting

In order to popularize e-voting, it is most important to prevent troubles due to mechanical failure. Some solutions have been gradually proposed, and the current measures are discussed below.

In November 2005, the Ministry of Internal Affairs set up the Research Committee on E-voting System[17] as a "permanent research entity that provides advisory functions from a professional standpoint regarding a way of an e-voting system, bringing new structure for improving reliability of the system into view." In March 2006, the Committee put together a report, "Basic Policy Regarding a Measure for Improving Reliability of E-voting System." The report stresses measures for trouble prevention in E-voting, addressing technical requirements of electronic voting devices and certification systems of technical requirements for improving reliability. It notes that there were three factors in past troubles: First, the contents defined by technical requirements themselves were inappropriate or insufficient; second, prior confirmation of whether an individual electronic voting device complied with technical requirements was not sufficient; and third, there were issues in operating the voting devices. Solutions to the first factor include the analysis of troubles from the past and a thorough investigation of the validity of the technical requirements, as well as the reinvestigation into the necessity of the legal binding power of technical requirements. For the second factor, it was suggested that the necessity of introducing a certification system should be examined in order to confirm compliance with technical requirements by third parties. For the third factor, it is important to follow through on improvement measures and to create manuals for those in charge of conducting the e-voting.

Traditionally, confirming compliance with technical requirements only involved self-inspection by manufacturers and joint inspection with an election committee at delivery to an implementing municipality. For self-inspection, manufacturers only had to submit a self-inspection certificate at the time of delivery. Thus the report noted that "instead of commissioning inspections to manufacturers and local public agencies, it is necessary to introduce a system of confirming compliance by third parties in order to prevent further occurrence of mechanical troubles and ensuring the reliability of E-voting system." The municipalities that have already conducted e-voting also suggested the necessity of a certificate system by third parties.

In response to the above report, on 18 December 2006, the Ministry of Internal Affairs and Communications issued the revised technical requirements and "Implementation Guideline for Confirming Compliance Regarding the Technical Requirements of E-voting System." Upon request for inspection by a manufacturer, a private inspection agency under contract with the Ministry is to confirm the compliance with technical requirements, and the result is to be publicized. It is an advantage for manufacturers to have e-voting devices with confirmed compliance as defined by the certification system. It is also true for each election committee or each municipality, since they can use devices of a certain technological level when choosing devices and implementing

[17] http://www.soumu.go.jp/main_sosiki/kenkyu/denshi_touhyo/index.html

E-voting. Basically, it is not only that a certification system can prevent unnecessary trouble, but also that it is indispensable. An inspection agency reports the results to the Ministry after the inspection and submits a “Report on Inspection and Verification of Electromagnetic Recording Voting System” to the Minister of Internal Affairs and Communications. The Ministry publishes the verification results upon receiving the report of the inspection results.

After the certification system was introduced in December 2006, Shiroishi City and Rokunohe Town held elections using e-voting on 22 April 2007. It was the third implementation of E-voting for both municipalities. The certification system was put into practice for those two cases, and E-voting devices that complied with technical requirements were used in the two elections. Until today, a couple of other cases of lections using E-voting have been held, and no significant cases of trouble have occurred.

Although the introduction of the certification system is useful for preventing troubles, what kind of and when an incident would happen will always remain unknown as E-voting involves devices. Thus manufacturers and governments are required to make constant efforts in the research and development of e-voting, as well as measures that envision various situations. Work is not completed once a system is established; revisions and improvements are required in e-voting, as in any other systems.

Lastly, the introduction of e-voting to national elections is mentioned here. As of December 2007, the Liberal Democratic Party and the New Komeito, which are the ruling parties, and the Democratic Party of Japan agreed on the introduction of E-voting to national elections. They worked to enact the bill in the Diet, and it passed the House of Representatives. However, it was withdrawn as an unfinished bill in the House of Councilors. At that time, the bill suggested that E-voting in national elections would be allowed only for municipalities with E-voting ordinances. However, the deliberation proceeded with difficulty around measures against the failure of voting devices, and time eventually ran out. Although the bill was withdrawn, it is notable that the introduction of E-voting was discussed officially. Furthermore, the fact that the bill passed the House of Representatives implies that there is some possibility of implementing E-voting in national elections. In Japan, the possibility of putting E-voting into reality seems to have been expanding gradually from local elections to national elections.

Bibliography

[An07] Anttiroiko, A. et. al. 2007. *Encyclopedia of digital government, 3 Vols.* Hershey: Idea Group Reference.

[Be06] Benz, A, et al. 2006. *Governance and democracy. Comparing national, European and international experiences.* London: Routledge.

[Co09] Contini, F. et. al. 2009. *ICT and innovation in the public sector. European studies in the making of e-government.* New York: Palgrave Macmillan.

[Da08] Dai, X. et al. 2008. *The internet and parliamentary democracy in Europe. A comparative study of the ethics of political communication in the digital age.* London: Routledge.

[Dr05] Drüke, H. et al. 2005. *Local electronic government. A comparative study.* London: Routledge.

[Fe00] Ferdinand, P. et al. 2000. *The internet, democracy and democratization.* London: Frank Cass.

[Gi03] Gibson, R. et al. 2003. *Political parties and the internet. Net gain?* London: Routledge.

[Gi04] Gibson, R. et al. 2004. *Electronic democracy. mobilisation, organization and participation via new ICTs.* London: Routledge.

[Ha00] Hacker, K. L. et al. 2000. *Digital democracy. Issues of theory and practice.* London: Sage, 2000.

[Ha99] Hague, B. et al. 199. *Digital democracy. Discourse and decision making in the information age.* London: Routledge.

[Hi98] Hill, K. et al. 1998. *Cyberpolitics. Citizen activism in the age of the internet.* Lanham: Rowan & Littlefield Publishers.

[Ho08] Homburg, V. 2008. *Understanding e-government. Information systems in public administrations.* London: Routledge.

[Iw04] Iwasaki, M. 2004. *E-voting* (in Japanese). Tokyo: Nihon-Keizai-Hyoron-Sha.

[Iw05] Iwasaki, M. et al. 2005. *E-democracy* (in Japanese). Tokyo: Nihon-Keizai-Hyoron-Sha.

[Iw09] Iwasaki, M. 2009. *E-democracy and e-voting* (in Japanese). Tokyo: Nihon-Keizai-Hyoron-Sha.

[Ke04] Kersting, N. et al. 2004. *Electronic voting and democracy. A comparative analysis.* New York: Palgrave Macmillan.

[Kh09] Khosrow-Pour, M. 2009. *E-government diffusion, policy, and impact. Advanced issues and practices.* Hershey: Information Science Reference.

[Mä04] Mälkiä, M. et al. 2004. *eTransformation in governance. New directions in government and politics.* Hershey: Idea Group Publishing.

[No01] Norris, P. 2001. *Digital divide. Civic engagement, information poverty, and the internet worldwide.* Cambridge: Cambridge University Press.

[Oa06] Oates, S. et al. 2006. *The internet and politics. Citizens, voters and activists.* London: Routledge.

[Pi00] Pierre, J. et al. 2000. *Governance, politics and the state.* New York: Palgrave Macmillan.

[Sh04] Shane, P. et al. 2004. *Democracy online. The prospects for political renewal through the internet.* New York: Routledge.

[To98] Toulouse, C. et al. 1998. *The politics of Cyberspace,* New York: Routledge.

[Ts98] Tsagarousianou, R. et al. 1998. *Cyberdemocracy. Technology, cities and civic networks*. London: Routledge.

Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
• seminars
• proceedings
• dissertations
• thematics
current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-299-4

EVOTE2012, the 5th International Conference on Electronic Voting, was held at Castle Hofen near Bregenz, Austria from July 11 to 14, 2012.
This volume contains 21 papers selected for presentation at the conference out of 44 submissions.
To ensure scientific quality, the selection was based on a strict and anonymous double-blind review process.

M. Kripp, M. Volkamer, R. Grimm: Electronic Voting 2012

205

GI-Edition

Lecture Notes in Informatics

Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm (Eds.)

5th International Conference on Electronic Voting 2012 (EVOTE2012)

Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

July 11-14, 2012
Castle Hofen, Bregenz, Austria

Proceedings

Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm (Eds.)

5th International Conference on Electronic Voting 2012 (EVOTE2012)

Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

July 11-14, 2012
Castle Hofen, Bregenz, Austria

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-205

ISBN 978-3-88579-299-4
ISSN 1617-5468

Volume Editors

Manuel J. Kripp, M.A.
E-Voting.CC GmbH, Competence Center for Electronic Voting and Participation
Pyrkergasse 33/1/2, 1190 Vienna, Austria,
Email: m.kripp@e-voting.cc
Prof. Dr. Melanie Volkamer
Technische Universität Darmstadt, Department of Computer Science
Hochschulstrasse 10, 64289 Darmstadt, Germany
Email: melanie.volkamer@cased.de
Prof. Dr. Rüdiger Grimm
Universität Koblenz-Landau, Institut für Wirtschafts- und Verwaltungsinformatik
Universitätsstraße 1, 56016 Koblenz, Germany
Email: grimm@uni-koblenz.de

Series Editorial Board

printed by Köllen Druck+Verlag GmbH, Bonn

Gedruckt mit Unterstützung des Bundesministerium für Inneres, Österreich

Preface

In 2004, the first Conference on Electronic Voting took place at Castle Hofen. Since then, the biennial EVOTE Conference has become the central meeting place for e-voting specialists. The interdisciplinary dialogue between academia, election experts and organizers, governments and politicians, as well as developers provides the foundation for fruitful discussions and intensive collaboration and exchange.

The fifth International Conference on Electronic Voting, EVOTE2012, is centered on the theme "Challenges for Electronic Voting – Transparency, Trust, and Voter Education". These challenges are addressed by sessions on verification, auditing, and coercion resistance.The conference provides an overview of the most recent research, technological developments, and practical experiences. The diversity and interdisciplinarity of EVOTE2012 is reflected in the 21 papers selected out of the 44 submissions based on a double blind-review process.

The submissions not only represent the wide array of technological developments and conclusive research currently taking place but also the worldwide support for electronic voting in places like Argentina, the United States, France, Norway, Turkey, and Switzerland. Nearly one-third of the accepted papers look at the latest practical implementations and the remaining two-thirds cover state-of-the-art academic research. Submissions were made by an equal number of new and experienced researchers including members of the International Programme Committee.

Special thanks go to the Council of Europe and the Gesellschaft für Informatik (German Informatics Society) with its ECOM working group on e-commerce, e-government, and security for their support and partnership in helping to organize the EVOTE2012 conference.

We would also like to thank the Lecture Notes (LNI) in Informatics editorial board under Prof. H. C. Mayr and the Gesellschaft für Informatik along with Cornelia Winter for their unconditional support in publishing the following articles in the LNI. We would also like to offer our gratitude to Jürgen Kuck from Köllen Publishers for helping us meet our print needs in such a perfect manner.

A big thank you to our conference partners, the Austrian Federal Ministry of the Interior and the Regional State of Vorarlberg, for their continued support. Further thanks go to our conference sponsors Everyone Counts, POLYAS, and Smartmatic for their efforts in helping create such a collaborative environment of exchange and discussion at EVOTE2012.

Finally, we would like to thank the reviewers and the members International Programme Committee who ensured the high quality of this publication with their knowledge and experience. Submissions of committee members and chairs were reviewed without their involvement.

Vienna, Darmstadt, Koblenz, July 2012
Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm

Co-organizers

E-Voting.CC GmbH
Competence Center for Electronic Voting and Participation

Council of Europe

Gesellschaft für Informatik
Working Group for E-Commerce, E-Government and Security

Introductory Words

It is clear for all of us that the power of individuals to communicate and connect has expanded in the last few years.

The World Economic Forum estimates that over two billion people are now online, nearly a third of humankind. There are 325 billion websites, 100,000 tweets per second and 48 hours of video clips uploaded to YouTube every minute.

The events of the Arab Spring reminded us of the growing appetite for information: A growing appetite for equality and for representative democracy.

The rise of electronic and social media has boosted the ability of cyber-activists to come together as a catalyst for change, to use the internet as a tool to counter heavy-handed governments.

New technologies have galvanised people to think and act more freely. In brutal societies such as Syria, activists and journalists increasingly operate websites rather than offices. They rally followers rather than staff.

What does this tell us?

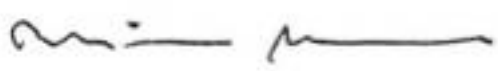
One thing is for certain. New governance models in a plugged-in world will no doubt entail greater demands for transparency and accountability.

New technologies are a challenge to the democratic process as we know it, but they also create enormous opportunities, and e-voting is one of them. However, in introducing new technologies to the electoral process, we must ensure that the legal, operational and technical frameworks fully comply with international standards and best practices for elections.

This is why the Council of Europe, already in 2004, responded to the new developments by adopting Recommendation (2004) 11 of the Committee of Ministers, a roundbreaking set of rules which still remains the only standard-setting instrument on e-voting.

But in a fast moving field such as this one, circumstances change as we speak. This is why the Council of Europe is always keen to engage in cooperation and exchange with government experts, other international organisations, civil society, business community and academics.

The 5th International Conference on Electronic Voting in Bregenz is an opportunity to exactly that – and we are looking forward to it.



Thorbjørn Jagland
Secretary General of the Council of Europe

Partners

Austrian Federal Ministry of the Interior

Regional State of Vorarlberg

Introductory Words

For the fifth time, Austria is hosting the International Conference on Electronic Voting. The industry-renowned "EVOTE" conference in Castle Hofen, Bregenz is a unique international forum for practitioners and researchers, students and instructors, and officials and policy makers, who all come together in order to discuss experiences, risks, and opportunities regarding the use of modern technology in elections and direct-democratic decisions.

"EVOTE2012" will specifically adress "Challenges for Electronic Voting – Transparency, Trust, and Voter Education". New technologies provide unique opportunities for communication and citizens' participation; they can bridge nations and peoples, helping to make this world a smaller place. At the same time, all electronic solutions that help facilitate the voting or participation process must also ensure security and transparency in order to gain the electorate's trust and acceptance.

Instruments of direct democracy enjoy increasing importance in countries around the world. People want their voices to be heard by politicians and lawmakers. The Republic of Austria has had a long and well-established tradition of direct democracy, especially with public initiatives (so-called "Volksbegehren"). For instance, the Federal Ministry of the Interior has recently initiated preparations for a far-reaching "democracy package." Within the framework of such a reform, specific participatory tools could be strengthened and the use of electronic technology certainly deserves further consideration.

On April 1, 2012 the European Union officially introduced its first participatory instrument, the European Citizens' Initiative. For the first time in the history of the Union, citizens are able to engage directly with EU politics. One million EU citizens from at least seven member states can now request a legislative act from the European Commission. The Citizens' Initiative not only provides the legal framework for collecting statements of support on paper but also via the Internet. This is a major step in bringing European democracies into the 21st century as it turns the European Citizens' Initiative into the first European-wide tool for "e-participation."

I consider it both exciting and rewarding to carefully watch future developments in this field and other areas of electronic voting and participation. Accordingly, "EVOTE2012" promises to offer fruitful discussions and indispensable information for representatives in academia, administration, and politics alike. My best wishes accompany the coming days, and I am looking forward to the conference's findings.

Johanna Mikl-Leitner
Federal Minister of the Interior

Sponsors

Smartmatic, Barbados

Everyone Counts, San Diego

POLYAS, Germany

Intersky, Germany

International Programme Committee

Programme Committee Chair

Manuel Kripp, Austria
Melanie Volkamer, Germany
Rüdiger Grimm, Germany

International Programme Committee

Mike Alvarez, USA
Harald Baldersheim, Norway
Frank Bannister, Ireland
Jordi Barrat, Spain
Josh Benaloh, USA
David Bismark, Sweden
Nadja Braun, Switzerland
Thomas Buchsbaum, Austria
Susanne Caarls, Netherlands
Chantal Enguehard, France
Simon French, United Kingdom
Paul Gibson, France
Kristian Gjosteen, Norway
Thomas Grechenig, Austria
Thad Hall, USA
Rolf Haenni, Switzerland
Catsumi Imamura, Brazil
Shin Dong Kim, South Korea
Norbert Kersting, Germany
Reto Koenig, Switzerland
Robert Krimmer, Poland
Monique Leyenaar, Netherlands
Ylle Madisse, Estonia
Laurence Monnoyer-Smith, France
Hannu Nurmi, Finland
Wolfgang Polasek, Switzerland
Julia Pomares, Argentina
Michael Remmert, France
Josep Reniu, Spain
David Rios, Spain
Fabrizio Ruggeri, Italy
Peter Ryan, Luxembourg
Mark Ryan, United Kingdom
Kazue Sako, Japan
Berry Schoenmakers, Netherlands
Robert Stein, Austria
Dan Tokaji, USA
Alexander Trechsel, Italy
Kristian Vassil, Estonia
David Wallach, USA
Gregor Wenda, Austria

Organization Committee

Maria Kellner
Gisela Traxler

Content

Session 5: Auditing and Testing of E-voting

Session 6: Practical Experience with Internet Voting

Session 7: Practical Experience with E-voting

Session 8: Analyzing E-voting: Survey and Results

Session 9: New Developments and Improvements to E-voting

Overview

Manuel J. Kripp[1], Melanie Volkamer[2], Rüdiger Grimm[3]

[1]E-Voting.CC GmbH
Competence Center for Electronic Voting and Participation
Pyrkergasse 33/1/2, 1190 Vienna, Austria
m.kripp@e-voting.cc

[2]University Darmstadt
Department of Computer Science
Hochschulstraße 10, 64289 Darmstadt, Germany
melanie.volkamer@cased.de

[3]University Koblenz-Landau
Institute for Information Systems Research
Universitätsstrasse 1, 56016 Koblenz, Germany
grimm@uni-koblenz.de

With the fifth EVOTE conference series the tradition of interdisciplinary discourse on electronic voting at Castle Hofen continues with articles from experts in academia, administration, politics and industry. The dialogue and sharing continues in 2012 with an impressive set of papers and presentations on various aspects of electronic voting.

This year's conference theme is c*hallenges to electronic voting: transparency, trust and voter education*. The 2012 proceedings consist of 21 papers selected in a double-blind review process from 44 submissions to bridge the gap between theory and practice ocvering topics like verifiability of Internet and electronic voting, coercion resistant voting systems, auditing and testing as well as mobile voting for sight-impaired citizens. The papers are clustered in nine sessions, which are presented in the following:

The **first session** looks the recent practical experiences with Internet voting in Norway and the implications on verification. Ida Sofie Gebhardt Stenerud and Christian Bull present the experiences and challenges of the election commission in Norway with the implementation of Internet Voting and the lessons learnt. Jordi Barrat, Michel Chevallier, Ben Goldsmith et al. evaluated the Internet voting in Norway and analyse in their paper the special feature of return codes to ensure voter verification in Norway.

The **second session** presents the technical perspective on Internet voting in Norway. The first paper by Jordi Puiggali and Sandra Guasch describes the technology behind the voter verification return-code scheme and analyses the implementation from a developer's perspective. Denise Demirel, Hugo Jonker and Melanie Volkamer investigate the mixnet used in Norway and propose a verification method to improve efficiency and privacy.

In the **third session** verification of electronic voting is discussed with an analysis of the e-voting system used Victoria, Australia by Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen and Zhe Xia. Maina Olembo, Anna Kahlert, Stephan Neumann and Melanie Volkamer look at the possibilities for verification in the online voting solution POLYAS.

Session four presents new research on coercion resistant e-voting systems. The paper by Oliver Spycher, Reto Koenig, Rolf Haenni and Michael Schläpfer proposes a verifiable Internet voting protocal that prevents voter coercion. Jerome Dossogne, Frederic Lafitte and Oliver Markowitch present how multi-party designated verifier signatures can be used a solution to provide coercion freeness in electrnoc voting schemes.

Session five deals with the growing challenges of auditing and testing of electronic voting systems. Michelle Shafer, Cyrus Walker, Jay Aceto and Edwin B. Smith propose a methodology for auditing of electronic voting systems. Mark Philips and Richard Soudriette discuss the importance of independent testing of electronic voting systems and the practical implication.

In **session six** practical experiences with Internet voting for citizens living abroad are presented and discussed. Ardita Driza-Maurer, Oliver Spycher, Geo Taglioni and Anina Weber present the experiences with Internet voting in Switzerland. Tiphaine Pinault and Pascal Courtade provide an inside look on the French Internet voting project for citizens abroad.

The **seventh session** presents practical experiences with electronic voting machines. First Carlos Vegas looks at the new e-voting machine in Belgium. Guillermo Lopez Mirau, Teresa Ovejero and Julia Pomares analyze the developments and implementation in Argentina.

Session eight presents the research findings on different analysis of the current status quo of electronic voting. Nina Boulus-Rødje maps the literature on electronic voting and highlights the importants topics of discussion. Jessica Myers and Joshua Franklin developed a classification structure of current and future voting technologies. Jurlind Budurushi, Stephan Neumann and Melanie Volkamer analyze the results of a survey on the use of smart cards to support the voting process.

The **ninth session** looks at new debates and developments in the field of electronic voting. Marc Teixidor Viayna analyses the consequences of null votes for electronic voting systems. Dalia Kader, Ben Smyth, Peter Ryan and Feng Hao propose a recovery round to enable the election result to be announced if voters abort, and adds a commitment round to ensure fairness. H. Serkan Akilli presents mobile voting as an alternative for blind voters. And Jonathan Ben-Nun, Niko Fahri, Morgan Llewellyn, Ben Riva, Alon Rosen, Amnon Ta-Shma, Douglas Wilkstrom report on the desing and implementation of a new cryptographic voting system, designed to retain the look and feel of standard paper-based voting systems.

Session 1

Verifiable Internet Voting in Norway: Lessons Learnt

When Reality Comes Knocking
Norwegian Experiences with Verifiable Electronic Voting

Ida Sofie Gebhardt Stenerud and Christian Bull

Norwegian Ministry of Local Government and Regional Development
P.O. Box 8112 Dep.
0032 Oslo
Norway
{ida.stenerud | christian.bull}@krd.dep.no

Abstract: This paper discusses the Norwegian experiences in piloting a verifiable, remote voting system in a legally binding, public election. First, we provide a high-level description of the system used. We then go into detail about the major challenges that were encountered in the implementation and execution of the system. In particular, the generation and printing of return codes and the key management are described in detail. We also discuss the relationship between the Norwegian Electoral Management Body and the system integrators, indicating how verifiability may enable new models of cooperation.

1 Introduction

During the municipal and county council elections in September 2011, Norway conducted trials using remote electronic voting. Ten municipalities participated in the trials, and the approximately 168.000 voters could vote online during the advance-voting period, lasting for 30 days. These trials were unique in that they – as far as we are aware– represented the first venture into coercion-resistant, verifiable, and remote electronic voting conducted by a national government. The Norwegian system is able to mathematically prove that recorded votes are counted correctly, and this is verifiable to independent third parties. In addition, voters get proof that their voting intent has been correctly recorded.

The purpose of this document is to provide a primary source of insight into the practical sides of piloting verifiable electronic voting. The intended recipients are the Electoral Management Bodies of other countries that may be considering piloting or implementing Internet voting. Some of the lessons learnt throughout the project have been painful, and by sharing them, we are hoping to make the road less rocky for the next country in line.

We also hope that these practical experiences are noted by academic protocol authors. Seemingly insignificant protocol design choices may have unexpected real-life consequences when implemented. Therefore, practical considerations need to be taken in protocol design.

In Norway, the Ministry of Local Government and Regional Development acts as the Electoral Management Body (EMB) and is responsible for electoral rules and regulations. While local authorities are usually responsible for actually carrying out the elections, the ministry took a more hands-on approach in the case of the e-voting pilot. Therefore, in this paper, the terms "EMB", "Ministry" and "e-vote 2011 project" will be used interchangeably.

2 Functional Overview of the Norwegian Electronic Voting System

From the voter's perspective, the Norwegian electronic voting system is fairly simple. The voter logs in using MinID, a widespread, well-known, and freely available two-factor authentication mechanism. Once verified, the voter is presented with a point-and-click interface showing the ballot. The voter makes her selections and submits them to a Java applet, which has already been downloaded to the voter client PC. The applet encrypts and digitally signs the vote and then sends it to the central voting servers.

Immediately after voting, the voter receives a text message containing a 4-digit number, from now on referred to as a *return code*. This return code can be compared to the voter's poll card. The poll card, which the voter receives by mail before the voting period begins, contains a list of all the available parties to vote for and their corresponding 4-digit code. The return codes are individually calculated per voter prior to the election. The return code in the SMS should correspond exactly to the chosen party printed on the poll card. This allows the voter to verify that the vote has been correctly received by the voting server, and is referred to as a cast-as-intended proof. If the codes do not match the option for which she voted, she will know that the vote has not been received correctly.

The voting process is illustrated in Figure 1 below:

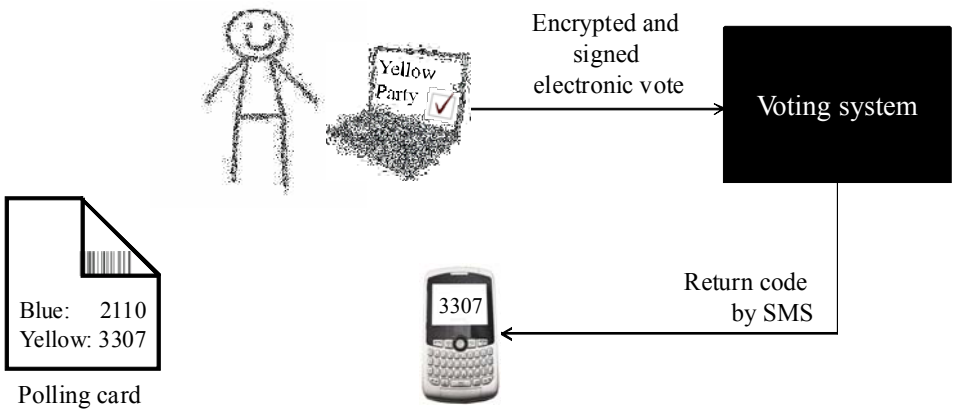


Fig. 1: A functional overview of the voting process

To mitigate the threat of coercion in Internet voting, voters are allowed to cast an unlimited number of Internet ballots, and even cancel the electronic ballot on by voting on paper. This feature is not discussed further in this paper. For more information, see [Gj10].

Why were the return codes sent via SMS and not just displayed on the screen? If a voter casts multiple votes, and the return codes were shown on the voter's computer, an attacker could learn the meaning of the return codes and replace the vote without the voter noticing. Therefore, the codes are delivered out-of-band.

Note that checking the return code is entirely optional and that the poll card is not used for authentication. Hence, a voter not in possession of the poll card can still vote, but will be unable to verify the SMS return code.

3 Return Codes Production: A Series of Unfortunate Events

The return codes form the first part of what is known as the Norwegian end-to-end[1] verifiable voting protocol (see Figure 2 below). Verifiability enables voters, election commissions, and election observers to verify the integrity of the election results and thus increase transparency and trust in the election [Ka11]. Such protocols are often seen as a measure to build voter trust.

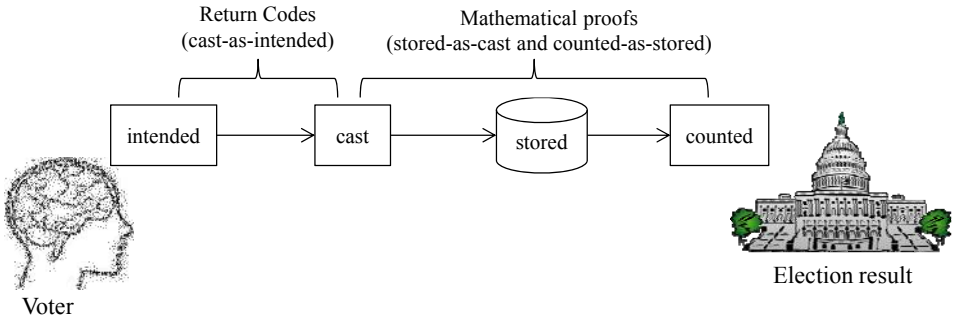


Fig. 2: The vote life cycle and the verification steps

The rationale behind implementing return codes in Norway was, however, somewhat different. The main purpose was to give the EMB the ability to detect systematic manipulation of client computers. In fact, the return codes were a solution to the requirement OS8.7 of the system requirement specification: *"Even though the e-voting client domain may be under outsider control, the e-voting solution shall be such that it is not feasible for an outsider to systematically manipulate the votes without detection"* [Ev09]. However, the fact that they also seemed to raise trust was a welcome side effect.

[1] The Norwegian use of the term "end-to-end verifiability" is somewhat controversial. However, the system enables verification of the entire life cycle of a vote, from end to end.

For the EMB to be confident that an attack would be detected, a certain percentage of voters would need to actually perform the check of their return codes. Though calculations of this percentage have not been published, they will most likely be similar to those published for the Pnyx protocol:

> *In an election with 40,000 ballots cast and a manipulation of just 1% of them, the chances of detecting the manipulation are more than 90% if just 230 voters verify. If 2% of the voters verify their ballots, the same manipulation is detected with a probability of more than 99.9%.* [Sc05]

At the time of writing, we do not have any estimates of the percentage of voters who performed the verification. However, to test the system prior to the pilots, the Ministry conducted several small-scale, non-binding test elections (so-called pre-pilots), with return codes used in two of them. According to data from a voter survey conducted by Synovate AS, an independent market survey provider, close to 90% report to have checked the return codes in these tests. Raw data can be found in [Ev11] (Norwegian only). Though one should be careful to generalize from this small sample, these are undoubtedly high numbers. Still, considering that return codes are pushed out to the voter by text messages, and require very little effort to check, the numbers are probably not so unrealistic when it comes to the actual pilot.

In general, return codes were well-received by voters. In-depth interviews indicated that voters found the return codes "confidence-inspiring", and some voters with disabilities mentioned how it gave them confidence that they had managed to cast their vote successfully. Interestingly enough, survey data from the pre-pilots that were conducted without return codes also showed that the majority of voters had high confidence in the solution. This is perhaps a symptom of the high level of trust in Norwegian elections.

3.1 Return Code Printing

Even though we received positive feedback on the simplicity of the cast-as-intended verification process, this was anything but simple to implement. The return codes created significant challenges in the generation and printing processes.

During the configuration phase, two data sets are created.

1) The voter list, containing all eligible e-voters
2) The return code sets. Each set consists of a list of parties and their corresponding 4-digit return codes.

Initially, the contents of these files are not linked, and no secret can be learned by the possession of just one of these files. However, the *relationships* (henceforth called "bindings") between individual voters and return codes are very sensitive. An attacker in possession of the return codes, the voter list, and the bindings, plus the ability to monitor

the SMS gateway, will be able to breach voter privacy. For an outsider, this would be nearly impossible to achieve. However, as the EMB is essentially in possession of all this data, great care must be taken to ensure that the EMB is never able to break voter privacy.

To ensure that the Norwegian EMB is able to learn the meaning of the return codes, the return code generation process generates an output encrypted with the public key of the printer service. The key pair is generated by the printer service, and only the printer service is in possession of the decryption key. Therefore, the EMB cannot learn the return codes. In addition, the bindings are created by the printer services during the printing process. This process is open to observation and in 2011 was observed by representatives from the EMB and the OSCE.

While this procedure ensures that the EMB is not able to violate privacy, the printing service is now in possession of uncomfortable amounts of data. To make sure that no single person or component is in possession of sufficient information to violate privacy at any time, printing is divided into two separate phases, each performed in a physically and logically separate printer environment. Figure 3 illustrates the process of printing return codes on poll cards.

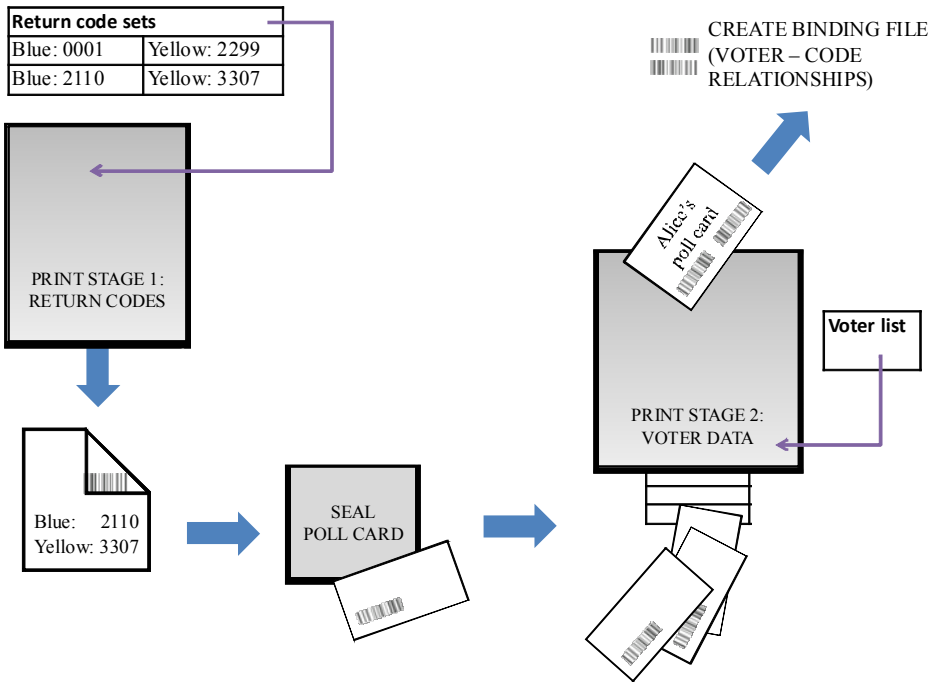


Fig. 3: The poll cards printing process

In print stage 1, the printer service randomly selects a return code set, and prints it on the inside of an A4 sheet. This sheet is then folded, sealed, and perforated so that the only thing printed on the outside is a bar code representing the ID of the return code set. During the 2011 pilots, in order to increase the opacity of the sealed poll card, the EMB used extra thick paper (120g) and coated the entire inside with yellow ink. The yellow ink also had the benefit of increasing contrast for improved readability; the thicker paper increased postage costs.

Once sealed, poll cards are manually shuffled and moved to print stage two, which is physically and logically separate from stage one and operated by different personnel. Here, eligible voters are picked at random from the voter list and their personal data printed on a poll card. The binding between voter and return code set is read from the bar code and subsequently written to file. This file is then uploaded by the EMB to the component responsible for sending out the return codes by SMS. This process ensures that no single person or component can ever know the meaning of the return codes relative to an individual voter.

Even though the print process was tested prior to the 2011 pilot, problems were encountered when it came to producing larger number of poll cards. While details are not entirely clear, we know that there were incidents where the actual poll card did not correspond to the information in the bindings file. This caused a few voters to receive the wrong return code after voting. Out of the approximately 168,000 poll cards that were produced, from which 28,001 voters actually cast an electronic vote, the support call centre received 74 reports from voters who received a return code that did not match their vote option [NS11].

While this might sound like a potential disaster, it did not cause any uncertainty in the integrity of the system. The EMB knew that if there had been any vote manipulation, the received return code would have corresponded to one of the other return codes on the voter's poll card. Anything else would have been mathematically impossible. Fortunately, for all the affected voters, the SMS return code never corresponded to anything printed on the poll card.

On a positive note, this provides a good indication that voters not only read and understand the return codes, but act as instructed when something seems amiss. If there was any sign of manipulation, the EMB would have encouraged the voter to cast a physical ballot and started an investigation. As electronic voting was only available in the advance voting period, any voters subject to manipulation would have had time to cancel their electronic vote by voting on paper on Election Day.

3.2 Challenges Posed by Security Controls

Running simultaneously with the e-voting system is an elections administrative system. Here, all the rules governing the election, such as municipal data, eligible party lists, and election opening hours are configured. The print files containing voter data and return codes are based on data from the administrative system. Because of late changes to the

administrative system, some eligible party lists were not included in the original print file. As these files were encrypted with the printer service public key, the Ministry was unable to check their contents for correctness. The missing data were discovered in an extraordinary check of the administrative system. At this time, the return code printing was going on, causing the entire first batch of poll cards to be discarded.

Before printing could be resumed, the Ministry had to re-generate return codes, a challenge in itself, as the infrastructure was unavailable due to the terrorist bombing only nine days earlier. The building in which the return code generation servers were housed was a crime scene and thus inaccessible to the Ministry. After a few days, the Ministry was granted special permission to evacuate the servers. When printing was finally restarted, there was only a matter of days before the opening of polls. At this point there was not enough 120g perforated paper available, so paper thickness had to be reduced to 90g.

In addition to the delay caused by the re-generation of return codes, the printer company had also discovered that the printing process was significantly slower than expected. All this leads to a mad rush in the printing of poll cards, with three shifts working around the clock for several days. On the morning when the system was to be made available to the public, printing was still underway for the two largest pilot municipalities. As the generation of the bindings file is part of the printing process, voting cannot commence before printing is finished. This led to a few hours delay in making the system available for voters in the two affected municipalities.

In addition to the 74 reports on incorrect bindings, the support call center received another 35 return code related calls.

- 11 voters reported not having received a poll card
- 5 voters who voted online reported not receiving a return code
- 4 voters received a poll card with the return codes smeared
- 1 person received two poll cards, one with the correct binding and one incorrect
- 2 callers reported having received return codes without having voted

Upon receiving the first reports on incorrect return codes, the Ministry conducted an investigation into what had happened. As part of this investigation, representatives of the Ministry personally called several affected voters. Interestingly, the voters reported not having lost trust in the system. Rather, they felt that it was their duty to do as instructed and inform the authorities of the incident. When informed of the problems with the printing, all affected voters appeared assuaged.

All in all, while there were certainly problems related to the return codes, the Ministry is very happy with its first experience in using them. If the piloting of Internet voting is continued in Norway, our advice to the Ministry is to continue the use of return codes even where they, from a security standpoint, may not be strictly required (for example, for expatriates or low-value elections).

As should be evident from the preceding text, the return code solution piloted in 2011 was not entirely perfect. For instance, the printing process definitely needs re-working. In addition, both the voter information material and the user interface must be improved in order to better educate voters.

4 Verifiability by Proxy

In Figure 2, the return codes only form the first part of the Norwegian verifiable protocol. The second part is performed without any voter involvement. This is an extremely important feature as the return codes only verify to the voter that her intent has been correctly captured. They do not verify whether the vote has been correctly stored in the database or that it will be counted.

An in-depth description of this last part of verification is beyond the scope of this paper but can be found in [Gj10]. In sum, the system allows a verifier to independently verify

1. That return codes have been sent for all received ballots
2. That all received ballots have been stored
3. That all stored, valid ballots have been included in the tally

The Norwegian voting infrastructure must provide these proofs of correct operation to the verifier. This ensures that neither malfeasance on part of the EMB, nor any software error (intentional or unintentional) will undetectably alter the vote once cast. The fact that these measures were implemented to form a verifiable system ensured a lot of good-will in the academic community and among IT experts. We strongly believe that this academic support was important in achieving wide-spread trust in the technical solution.

4.1 The Effect of Verifiability in Trusting Infrastructure

As ever, the advantages of verifiability were not only apparent in building trust. An extremely positive side effect of verifiability was the fact that the EMB did not have to put complete trust in the counting infrastructure: the integrity proofs of the cleansing, mixing, and decrypting would reveal any irregularities.

Counting of electronic votes is extremely critical and even small errors can have dramatic consequences. It therefore seems common practice in electronic voting to use new servers for counting. Configuration and use of these is then performed under strict supervision. Considering the extensive number of certificates, keys, and passwords that need to be correctly in place for the Norwegian counting infrastructure to even operate, an untested infrastructure was unlikely to work on the first go. However, since the verifiable properties of the system allow, without any risk, the re-use hardware, the Ministry was able to perform test counts on the production system as late as Election Day to ensure that all components were functioning correctly.

In other words, the EMB itself has a clear self-interest in, and much to gain from, implementing verifiability in the system it deploys. This does not appear to be a motivation for most academic protocols, but has been a boon for the Norwegian government. On the other hand, verifiability is both computationally expensive and complex to implement. Though it is difficult to give an estimate of the extra development effort, it obviously raises the price.

4.2 The Legal Impact of Verifiability

Verifiability means that any manipulation or system error related to the processing of votes will be discovered. However, one can only know this once the election is finished. An obvious question is how to proceed if the proofs indicate irregularities. In the Norwegian e-voting pilot, the protocol would have been the same as in any electoral irregularity: the government would conduct an investigation. If the problems were shown to possibly have affected the election outcome, an option would have been to invalidate the results and call a second ballot. Note also that not all verification is performed after the e-voting period is over. As cast-as-intended verification is performed during the voting period, this would allow the EMB to detect irregularities during the advance voting period and act accordingly.

Even though an invalid proof would certainly have been unpleasant, it is still better than the worst-case outcome – an illegitimate winner of the election.

5 The Challenges of Key Management

Though not strictly related to verifiability, it's safe to say that one of the major challenges for the e-vote 2011 project was key management. To ensure integrity of the information flow, all communications between the different components were signed by the originating server and the signature verified by the recipient. The configuration phase creates, among other things, 15 different key pairs per election event, each consisting of a private key, a public key, and a password for the private key. Ensuring that each server had the correct files, when each component consisted of up to 10 servers, was a complex task.

For increased security, the passwords protecting the cryptographic keys were only held in the memory of the server. This means that restarting a server, or just the application, would require the passwords to be re-uploaded. If any one server lacked just one password, it would not have been possible to cast a vote using this server. For instance, if one of the ten RCG servers lacked a password, voters would have experienced intermittent failure when casting their votes (approximately one in ten votes).

This creates an additional challenge: How to gain 100% confidence in the correct functioning of the system before the opening of the election? The answer is that although the system vendor developed sophisticated "health checks" for the infrastructure, it was not, strictly speaking, possible. As one of many controls to assure that no one could cast a vote before the actual opening of the voting period, the system had a built-in scheduler that prevented this. It was therefore not possible to verify that votes would be accepted by the system before opening the election and the correct return codes calculated.

This was a typical paradox encountered several times: the strict security controls gave great confidence that no malfeasance could occur, but at the same time they also reduced the ability to test the system. This is one of the great dilemmas of secure electronic voting, and even within the e-vote 2011 project group there has been some disagreement on which property is more important.

5.1 Key Management and Separation of Duties

Cryptographic key management is a very challenging undertaking. One thing is the secure storage of secret keys; another is access control to those same keys. Typically, a small number of people both create the keys and have access to critical infrastructure. The only remedy for this is the separation of duties on the organizational as well as the technical level. In a small and fast-paced pilot project, this is, for all practical purposes, impossible to implement but will be a vital development in more mature electronic voting.

As part of the system design, a significant amount of separation of duties was implemented to ensure that critical secrets were kept apart. For instance, 4 laptops, 10 servers, 45 hard drives, and countless USB flash drives were used in the configuration. Even though separation of duties was implemented on system level, it proved difficult to implement similar controls at the personnel level. This was partly due to delays in the delivery of software, which created an unpredictable situation. To alleviate this problem, the EMB identified the most critical keys and secrets and created procedures to ensure that these were safely kept secret and separate. Despite the EMB's best intentions, the actual separation of duties is difficult to verify for an outsider. This would either require long-term observation or very advanced high-security storage equipment.

6 Does the EMB Need Complete Ownership of a Verifiable System?

The Norwegian approach was to assume as much ownership as possible, in order to ensure transparency and public trust. The software vendor was used only for development. On the negative side, assuming ownership means assuming risk. However, the buck will always stop with the EMB, regardless of contractual responsibilities.

It appears to us that end-to-end verifiability may in fact reduce the need for EMB ownership and involvement in the e-voting system. The fact that the processing of votes is independently verifiable means, that the EMB can safely transfer more operational responsibility to external parties, such as the software vendor or data center operator. Some of the challenges encountered by the Norwegian pilot project, such as key management and true separation of duties could have been more manageable with such an approach.

While a verifiable e-voting system may allow the EMB to take a somewhat more relaxed approach to operations, it does not reduce the need for close cooperation with the vendor. Even with small-scale piloting, an Internet voting project demands extensive development of the actual e-voting systems and the legal requirements to conduct such an election. The customer must always assume full responsibility for specification and testing and ensure that the system is, in fact, truly verifiable.

7 Further Research

We would certainly not argue that the Norwegian protocol is perfect. Certain identified threats have not been fully mitigated. For instance, we are not aware of any way to prove that the SMS received by the voter was in fact sent by the authorities. It would be beneficial if the veracity of the SMS could be proven to the voter and the EMB.

Independent researchers have also conducted a series of lab tests trying to exploit the weakest link in the protocol – the voter. In these experiments, test voters were presented with a malicious web site that changed the vote before encryption. Such a web site will never be able to calculate the correct return code, but it could undetectably steal the vote if the voter fails to notice any irregular behaviour. In one of the experiments, the malicious site tricked the voters into both 1) typing in the return code of the chosen vote option and 2) ignoring the fact that they received two text messages – one of them with a "wrong" return code. Disturbingly, none of the test subjects detected the deviation from the protocol [Ol11]. Further research is needed to understand whether or not these results can be applied to actual voting situations. What is certain, however, is that the protocol only requires a very low number of voters to notice irregularities in order for the EMB to detect an attack.

Another hypothetical "attack" is that a group conspires to falsely report wrong return codes. Since it would be impossible for the ministry to know whether reports are truthful or not, this would be a very difficult attack to defend against. One possible defence would be for the EMB to visit every person who reports wrong return codes and physically test their computer. Because the Norwegian EMB is represented by the local government in the municipalities, this would have been feasible but legally and politically unacceptable.

Additionally, the protocol, as it currently exists, makes the rather strong assumption that the vote collector server (VCS) and return code generator (RCG) will not cooperate to violate privacy. On one hand, this is an uncomfortably low number of actors required to guarantee privacy. On the other hand, maintaining even two different operating sites introduced significant unwanted complexity, as described in chapter 5 above. From the EMB's point of view, reducing complexity would be desirable.

8 Concluding Remarks

After reading this paper, the reader might question whether verifiability is worth the time and effort, when trust in the EMB is already high. We contend that the best, and quite possibly only, way to gain trust in the academic community is to implement a verifiable system. Support from the academic community will probably not in itself create trust among the general public. However, a good relationship with the academic community at least reduces the danger of a sudden mistrust of the technical platform.

Furthermore, verifiability is confidence-inspiring for the EMB. While the security measures implemented in the Norwegian e-voting system may appear difficult to live with, the challenge was temporary and most evident during the configuration phase. Once the system was up and the votes were coming in, the benefits became apparent in the very high confidence in the system. Also, piloting a brand new system of some complexity will always be demanding and somewhat chaotic. If piloting electronic voting is continued in Norway, we believe that the process will go more smoothly.

Procuring an E2E verifiable electronic voting system is not a simple task. This is a question of having the right resources available, both in terms of money and personnel. Hence, one should be weary of organisations without sufficient resources piloting electronic voting, as maintaining trust in electoral processes is of great importance to any democracy.

In this paper, we have indicated that with end-to-end verifiability the EMB may be somewhat more relaxed regarding the ownership of the election system and infrastructure. However, this only holds as long as the system is well tested. The Norwegian EMB in no way regrets taking on an active role as customer. The EMB must always assume full responsibility for specification and testing, in addition to ensuring that the final system is, in fact, truly verifiable.

An uncompromising outlook on security can be painful. However, we believe that it's a worthwhile cause. In many countries, the alternative will be distrust from the stakeholders. Verifiability is an important component in such an election, increasing the confidence in the EMB and of the stakeholders during and after the election. However, the intense testing required before the election is one drawback if the necessary resources are unavailable.

Bibliography

[Ev09] The Norwegian E-vote 2011-project, SSA-U Appendix 2B Requirements Table, 2009
http://www.regjeringen.no/nb/dep/krd/prosjekter/e-valg-2011-prosjektet/tekniskdokumentasjon/spesifikasjoner-tilbud-kontrakter.html?id=612121 [February 17th 2012]

[Ev11] The Norwegian E-vote 2011-project, Evaluering av testvalg høst10/vår11, 2011
http://www.regjeringen.no/nb/dep/krd/prosjekter/e-valg-2011-prosjektet/evaluering/evaluering-av-testvalg-host10var11.html?id=653612 [February 17th 2012]

[Gj10] Gjøsteen, K.; Analysis of an internet voting protocol, 2010
http://eprint.iacr.org/2010/380 [February 17th 2012]

[Ka11] Karayumak, F.; Olembo, M.; Kauer, M.; Volkamer, M.: Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System. Presented at EVT/EWOTE'11, 2011
http://static.usenix.org/event/evtwote11/tech/final_files/Karayumak7-27-11.pdf [February 17th 2012]

[NS11] Nore, H.; Stenerud, I.: The good, the bad and the terrible of verifiable electronic voting, VoteID 2011, 2011.

[Ol11] Olsen, K.: Alle ble lurt i falskt e-valg. Published in Teknisk Ukeblad 2011 (31), p. 20-21

[Sc05] Pnyx.core: The Key to Enabling Reliable Electronic Elections. A Description of Scytl's Cryptographic e-Voting Security Software, 2005
http://www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf [February 17th 2012]

[SVK11] Spycher, O.; Volkamer, M.; Koenig, R: Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting, VoteID2011, 2011
http://www.regjeringen.no/upload/KRD/Prosjekter/evalg/vedlegg/paper_transparency_and_technical_measures.pdf [February 17th 2012]

Internet Voting and Individual Verifiability: The Norwegian Return Codes

Jordi Barrat[1], Michel Chevallier[2], Ben Goldsmith[2], David Jandura[2], John Turner[2], and Rakesh Sharma[2]

[1]EVOL2 / eVoting Legal Lab
University of Catalonia / URV
Av. Catalunya, 35, Tarragona (Catalonia) 43002
barratj@tinet.org

[2]International Foundation for Electoral System (IFES)
1850 K Street, NW, 5th Floor,
Washington, D.C. 20006
rsharma@ifes.org

Abstract: The Norwegian return codes, used within an Internet voting project piloted in September 2011, intend to simultaneously achieve both receipt-freeness and individual verifiability. They are delivered as text messages with a code representing the value of a voter's cast ballot, but, according to the Norwegian Government, they would not breach the principle of secrecy, and they are not voting receipts, since the voter could always cancel the vote. However, some international electoral standards, like the *Recommendations on E-voting* from the Council of Europe, clearly forbid an Internet voting system that enables a "voter to be in possession of proof of the content of the vote cast." This paper analyzes the extent to which the Norwegian system complies with this standard and it concludes that there is no contradiction in using a teleological approach.

1 Introduction

Verifiability is one of the key issues that any Internet voting project has to address. As with other remote voting channels (e.g. postal voting), it does not normally provide a voter with any proof that his or her was cast or received as intended. In fact, receipts that can be used to prove the content of a vote are prohibited by some international electoral standards[1], as they facilitate the coercion of voters and vote buying practices.

[1] We will focus our attention on the following recommendation issued by the Council of Europe: Recommendation REC(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 / Legal, Operational and Technical Standards for E-voting. Available at: www.coe.int/democracy [April 24th 2012].

However, voting receipts are still a technically feasible solution and would improve the system's trustworthiness, provided they manage to overcome the problems concerning the secrecy of the vote and the freedom of the voter. While some countries (e.g. the Netherlands) decided to include voting receipts despite their negative effects over such principles, other projects, like the Norwegian one, intend to use voting proofs in a way that does not violate the principles of voter freedom or secrecy.

After a brief outline of the Norwegian Internet voting system (§ 2), this paper will focus on the so-called return codes (§ 3), that is to say, text messages that provide individual verifiability within non-supervised environments. Such mechanisms obviously challenge voting secrecy and freedom principles, but the Norwegian solution intends to overcome both problems with a multiple-voting scheme (§ 4). Finally, this paper will discuss to what extent such codes should be categorized as voting receipts (§ 5) and, therefore, to what extent they meet international electoral standards, like the recommendations from the Council of Europe, which prohibit the provision of such receipts to voters.

2 A Brief Outline of the Norwegian Internet Voting System

Norway piloted Internet voting for the first time during its municipal and county elections in September 2011. It was the first binding and official use of Internet voting after several trials during the period of technical and legal developments. Ten municipalities were selected to conduct the pilot, and after a broad evaluation and a general political assessment are carried out in 2012, the Norwegian Parliament – *Stortinget* – will decide whether or not to continue using Internet voting in future elections.

Internet voting was only used as a supplementary channel for casting a vote and was available for one month during an advance period of voting ending on the Friday before election day. Voters in the pilot municipalities were also able to use traditional paper-based ballots, which were available during the early and advance voting period and on election day (Ri11).

Norwegian electoral authorities conducted detailed assessments on how other countries had addressed the challenges generated by Internet voting and decided to both adopt some of the measures used by other countries and to include new features aimed at improving existing Internet voting solutions. As in Estonia, the Norwegian solution allowed repeat voting, whereby voters could cast repeated Internet votes. Internet voters were also able to cast paper votes during the early and advance voting period or on election day.[2] The final tally of votes only included the last Internet ballot (I-ballot) cast, unless a paper-based ballot (p-ballot) was cast, in which case the paper ballot was counted and the I-ballots discarded.

[2] The Estonian Internet voting system does not allow Internet voters to cast a paper ballot on election day, but apart from this the same possibilities are available in Estonia.

Transparency was another issue that the Norwegian electoral authorities intended to qualitatively improve in regards to previous Internet voting systems [see SVK11]. While other countries face criticism regarding the way they handle electoral information, Norway requires open-source programs, and its Internet voting project is based on a general license that enables anybody to download both the source code and other relevant documentation for non-profit purposes. The government also claims that all the information linked to the project is published.

Finally, the ability to verify that the system accurately reflects the will of the voters in the results that it produces is a common source of concern for Internet voting systems. Norway claims that its Internet voting system can be submitted to a software independent End-to-End (E2E) verification that, *inter alia*, includes Zero-Knowledge Proofs (ZKP) for the final cleansing and mixing stages. Moreover, Norway includes the so-called return codes, whose purpose is to allow individual verifiability that the Internet voting system has received the vote as cast by the voter from the voting client. The next section (§ 3) will describe such codes and the following section (§ 4) will assess how such codes may comply with electoral standards that do not allow voting receipts for remote voting channels.

3 Internet Voting, Individual Verifiability, and the Norwegian Return Codes

The return codes used in the Norwegian Internet voting system were simply text messages sent to the voter immediately after he or she had cast a ballot. The message included a code representing the party list that the voter had cast a vote for and indicated the number of personal votes that had been cast. An SMS message was sent each time an Internet vote was cast. Before the election, each voter received a polling card containing a list of codes for each party list on the ballot for the municipal and county elections. The combination of codes assigned to the party lists on the ballot was unique for each voter. Therefore, when the voter received the SMS message with the relevant code, he or she could refer to the polling card to determine whether the code represented the cast ballot. If the code did not match, representing a clear technical flaw in the system, the overall electoral process could continue because the voter would still be able to cast another I-ballot, which would hopefully be recorded correctly; the option to vote by paper ballot would have also been an option.

Such codes clearly improve the verifiability of the voting system as they provide proof that the system received the vote as cast and that it was cast as intended. However, it is only a partial verifiability because return codes do not prove that the vote is stored as cast or that it is included in the count as it is stored. However, the E2E mechanisms mentioned above intend to complete this sequence of verifiability encompassing all the electoral stages. With the challenges that these return codes generate in mind, the following sections will analyze how the return codes address the protection of the secrecy of the vote (§ 4) and to what extent they comply with the standards that preclude the use of voting receipts for remote voting projects (§ 5).

4 Return Codes and Vote Secrecy

Regardless of whether return codes are used or not, Internet voting always entails serious concerns about the secrecy of the vote and the freedom of the voter. This voting channel is normally used in uncontrolled environments, that is to say, a situation in which there are no means to guarantee that the voter is free from external influence in casting his or her ballot. There is no voting booth to ensure secrecy or official supervision to ensure that the voter is alone when voting, and therefore the vote might be submitted under pressure from external forces, which would breach both to the voter's freedom to vote as well as the secrecy of the vote[3].

Return codes only serve to strengthen these concerns. These SMS messages would simplify the task of coercers and vote-buyers because they need only ask the voter to provide the appropriate proof generated by the Internet voting system itself. Unless the voter manages to send a faked SMS message, which is difficult to do because they are sent by the server itself, the coercer would not be compelled to directly supervise the voting session to know how the voter cast his or her ballot.

Taking these risks into account, most Internet voting projects do not include individual verification means. They assume that the advantages linked to remote voting channels (e.g. easier access to the voting process for some groups) justify not being able to replicate some guarantees that exist in supervised voting environments (e.g. direct supervision). From this point of view, Internet voting can be seen as similar to postal voting. Postal voting is allowed in many Western democracies; despite being unable to guarantee the freedom of the voter and the secrecy of the postal votes cast, it is seen as a legitimate voting channel[4]. Postal voting does not provide any means by which the voter can individually verify that his or her vote has been received or counted as cast. While Estonia and some Swiss cantons (e.g. Geneva) use such an approach, the Netherlands and Norway sought to implement Internet voting with mechanisms for individual verification.

The *Rijnland Internet Election System* (RIES) project was canceled as a result of the overall re-evaluation conducted by the Dutch electoral authorities after weaknesses discovered by an NGO in electronic voting machines previously used in the Netherlands. The cancellation of the Internet voting system was a side effect of these concerns as the main criticism was related to electronic voting machines and not the Internet voting channel.

---

[3] In Norway, such prevention is even more important due to previous incidents where members of some minority groups were thought to have exercised undue influence over some voters. See [Sm10] for a detailed assessment on how Internet voting would not meet electoral principles directly linked to the secrecy of the vote.

[4] The Venice Commission issued a report [Ve04] where both postal and Internet voting, as remote channels, were assessed to determine whether they complied with international electoral standards. The Commission concluded that they did meet international standards provided that certain features were included, but that individual verification was not one of the requirements that any voting channel needed to include.

Despite this, the RIES project's verification mechanisms are worth noting. Once an Internet ballot was cast, the REIS system provided the voter with what was called a 'technical vote', which was an encryption code for the vote cast. When all voting was completed, the election authorities published a list of the codes used with an indication of the ballot option made for each technical vote. This allowed for individual verifiability by the voters, who could see that their vote was recorded correctly, as well as universal verifiability, as anyone could verify the overall results of the Internet votes by tallying the votes for each ballot option.

This feature was seen as a great innovation because it provided the voter with a means to directly verify a process that is normally opaque for the average citizen. However, these advantages also had a critical trade-off with serious implications for the secrecy of the vote. As the OSCE/ODIHR recalled, "if a voter ... discloses his authorization code and his technical vote, anyone can determine his/her actual vote by simply trying all the candidate identities until a match is obtained" [Os06: 15; see also Jo07: 20-25]. The technical vote would no longer be a neutral code as it would reveal the value of a given ballot while also linking the vote to an individual. Therefore, within this schema, individual verifiability would only be feasible when accepting that the secrecy of the vote could be breached in a way that is not possible with postal voting.

The Norwegian project took into account the Dutch experience and tried to address such challenges through repeat voting. The argument is that the voter is able to cast as many ballots as he or she wants, either by Internet or by paper means, with only the last Internet vote or the paper vote being included in the results. The coercer would therefore have no way of knowing if the ballot cast in his or her presence or the return code presented to him or her represented the ballot that was actually counted for that voter.[5]

While Estonia has multiple voting and the Netherlands individual verifiability, Norway mixes both features as a way to simultaneously achieve two goals: a sound protection of the secrecy and freedom of the vote and individual verifiability (or at least a limited version that intends to guarantee that each ballot is received as cast and cast as intended). Return codes do offer proof linked to a certain ballot, but, due to repeat voting, there is no way to check which ballot is included in the final tally [see Bu11: 17-20].

[5] This argument is not without its critics. Repeated Internet ballots might also be tracked by the coercer, as he or she could retain the control over the mobile phone that receives the return code, Internet ballots cast during the very last stage of the voting period would preclude the chance to revoke them by another Internet vote and finally, as recalled by Eivind Smith, the social context may also become a key feature. Although theoretically any voter can freely go to a polling station and supersede a previous ballot, "(other) members of the social structure that is the source of the problem would easily be able to discover and report attendance at a polling station" [Sm10: 12 (edited version)]. Therefore, from this point of view, neither repeated Internet ballots nor paper votes would be good solutions to overcome the problems that return codes create for the secrecy of the vote. However, a comparative perspective, which would take into account how other voting channels (e.g. postal voting, supervised polling stations) protect this legal principle, might emphasize the advantages of having multiple options to cast a ballot.

Moreover, there are also concerns about the anonymity of the vote when return codes are in use. It is worth questioning how the application can send specific data about the value of a voter's ballot while maintaining the anonymity of the vote. Following the explanations of the Norwegian authorities, such a paradox is solved through crypto architectures [see Gj11 and Gj10]. The ElGamal system allows the return code generator (RCG) to establish a dialogue with the vote collection server (VCS), retrieve enough data about a ballot, and send back the relevant code without breaching anonymity. It relies upon an extremely complex crypto systems, but it is worth recalling that even without such return codes, many Internet voting projects also include digital signatures that protect anonymity with double envelope methods. Therefore, ElGamal only represents a more developed crypto system that also allows the delivery of return codes in order to provide a level of individual verifiability.

5 Return Codes as Voting Receipts

Once accepted that the provision of return codes, allowing for individual verifiability in a manner that still protects the freedom and secrecy of the vote, could be a solution for some Internet voting projects, there remains a legal barrier as some international electoral standards prohibit voting receipts when using remote voting channels. The Council of Europe's *Recommendations on E-voting* is a good example as the 51st recommendation states, that "a remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast".

While the Council of Europe recommendations are precisely that, only recommendations, they have a special legal status for the Norwegian pilots as they were incorporated into the electoral legal framework through the Regulation Relating to Trial Electronic Voting. Faced with such a clear statement in recommendation 51[6], it is worth wondering to what extent the Norwegian return codes manage to comply with these standards. Although the Norwegian solution might be valid from technical and social perspectives, a legal assessment is always necessary and such standards clearly identify a potential problem[7].

[6] Moreover, other recommendations also seem to reject the use of return codes. The 17th recommendation requires anonymity of the ballots being inserted into the ballot box and "that it is not possible to reconstruct a link between the vote and the voter". The 35th recommendation emphasizes the same goal requiring that "votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum". Finally, the 19th recommendation includes a general statement regarding the protection of secrecy while managing electoral information. While the 35th only requires conditional ballot secrecy, that is to say, a feature that may be breached under some circumstances, the other two require absolute secrecy [see Jo04].

[7] The Norwegian legal framework also requires an electoral system with "frie, direkte og hemmelige valg" (§ 1-1 Election Act; translation: free, direct and secret elections; see also § 10-5), but the system did not foresee individual veriability for remote voting channels. Citizens using postal voting did not receive a proof of content of his/her vote.

The Council of Europe recommendations are accompanied by an explanatory memorandum, that helps to interpret and contextualize the recommendations. The memorandum does not specifically discuss the option of individual verification for remote voting in unsupervised environments. However, when it analyzes the risks linked to the web application, the browser, and the software, some comments can clearly be applied to the Norwegian return codes: "The web application should not allow the user to retain a copy of his or her vote. This means that the application should not offer the functionality of printing, saving or storing the vote or (part of) the screen on which the vote is visible ... At the very least, there should be no storing of information [by the browser] after the voter has finished casting the vote."

Despite not explicitly prohibiting text messages sent back to the citizen by the voting servers, it seems obvious that the Norwegian return codes are an analogous scenario and it is necessary to assess whether they comply with this recommendation from the Council of Europe.

The Norwegian Government claims that its Internet voting project meets this requirement as return codes should not be understood as voting receipts [Bu11: 20]: they would not be able to provide proof of the content of the vote cast because the voter always has the chance to substitute such a ballot with another I-ballot or with a p-ballot (which may have even been cast earlier than the I-ballot). A return code would not be a voting receipt, whose use is forbidden according to the *Recommendations*, and therefore this recommendation would pose no problem for the implementation of the Norwegian Internet voting project.

To our understanding, such an interpretation is hardly acceptable. As explained in the previous section, a return code is always linked to a set of codes that had been given to each voter in conjunction with his or her polling card. Given that each code refers to a given candidature, the return code is disclosing the content of this ballot and suffices as "proof of content of the vote cast". The fact that such a ballot might not be the final one included in the tally would not be important for the following reasons.

First of all, (i) it is worth noting that the wording refers to the vote "cast" and not to the vote "tallied". A scenario based on repeat voting allows several votes to be cast by the same voter, with only one being finally tallied. Each ballot cast (not yet tallied) will generate the relevant return code that will disclose the value of this ballot. It will therefore function as proof of content of the vote cast.

Moreover, even if we prefer not to make a distinction between votes cast and tallied[8], there is another argument (ii) against the compliance of the Norwegian return codes with this recommendation. Given that the wording only refers to the voter, and not to third parties, it is obvious that the voter will know which one of the votes cast would be the final one included in the tally. Therefore, at least one of the return codes would be a full proof of content of a ballot cast and also tallied.

[8] The system would *receive* several ballots, but only one will be finally *cast/tallied.*

If the voter cast a p-ballot, the return code would never be linked to a ballot finally tallied, but the previous explanation would still be valid for those voters only casting I-ballots and therefore, at least for this group of voters, return codes would offer full proof of the content of a vote cast and also tallied, precisely what the recommendation intends to forbid.

Finally, (iii) if the return codes are not voting receipts, as the Norwegian government states, it is worth wondering what their purpose is. Theoretically return codes are thought to enhance individual verifiability, but, if they cannot provide proof of the vote being cast, there will be no verification, and they become meaningless.

To our understanding, the Norwegian return codes do provide proof of content of the vote being cast and therefore an initial assessment would likely find that they do not comply with the 51st recommendation from the Council of Europe. However, there are other ways to approach this issue and, as we will discuss below, return codes may meet the Council of Europe's recommendations provided we adopt a less literal interpretation of their wording.

Hermeneutic theories argue that literal interpretation is not always the best way to understand the actual meaning of legal rules and that it is necessary to balance literal interpretations with other points of view. Historical, systematic, authentic, and teleological methods are normally used to discover the intended meaning of a rule and to achieve its fairest implementation [in general, see Al83].

Regarding the 51st recommendation of the Council of Europe, where a literal method clearly leads to a breach when using return codes, it is worth using the teleological strategy in order to discover the actual purpose of the recommendation. The key point consists in making a distinction between the role of the voter and that assumed by third parties[9]. As we have seen above, the voter will always know whether the return code is a real voting receipt, that is to say,, proof of content of a ballot cast and tallied, but, thanks to multiple voting chances, third parties will never have the same certainty that a given return code actually represents the vote that will be tallied. They will never know whether a return code has been canceled by another I/p-ballot. Only the voter knows this, and he or she has no way of proving it.

Following this reasoning and taking into account the wording of the recommendation, the Norwegian system does not provide *at least to third parties* a proof of content of the vote cast. The voter does receive such proof but not third parties.

If we follow a literal method of interpretation, such a distinction has no impact because the recommendation only refers to the voter and not to third parties. It forbids providing proof of content to the voter and as we have already seen that return codes only meet this

[9] Please note that this meaning of third parties does not include backend users. They will always be able to reveal the content of a given ballot, but a proper separation of duties as well as other technical safeguards would address this risk. On the other hand, other types of third parties, like relatives or similar potential coercers, may use return codes in order to reveal the value of a given vote, but in this case, both a proper separation of duties and other technical safeguards would be meaningless.

requirement with respect to third parties but not the voter. Douglas Jones reached the same conclusion when assessing whether some e-voting systems may comply with this recommendation: "This rule prohibits cryptographic systems such as that being developed by VoteHere (Andrew Neff and Jim Adler) and SureVote (David Chaum). These systems prove to the voter, in the privacy of the voting booth, that the receipt contains their vote, but they do not provide, to the voter, sufficient information to prove to anyone else how they voted, using that receipt" [Jo04] [10].

However, using a teleological method, we will easily discover that the recommendation does not forbid a proof *only* given to the voter. What it actually rejects is a proof that might be given to third parties in order to verify whether the voter has correctly followed the instructions by someone trying to coerce a voter or buy votes. If the return code only provides information, which is only valuable to the actual voters, its data is not dangerous for maintaining key electoral principles like the secrecy of the vote and freedom of the voter. Obviously return codes can always be given to third parties, but with multiple voting options, they are rendered meaningless to those parties because the return codes do not show further votes or cancellation of the vote. Such limited use of return codes would create no concerns while significantly enhancing individual verifiability[11].

McGaley and Gibson share this opinion and their approach is quite interesting because they intend to restructure CoE's document in its entirety, aiming to minimize its internal contradictions. In their analysis of both the secrecy of the vote and the 51st recommendation, their final suggestion adds slight nuance to the literal wording of the Council of Europe's recommendation. Significantly, Mcaley and Gibson's revision of the 51st recommendation includes the difference between the voter and third parties, which did not exist in the original: "The voter shall not be allowed to retain possession of anything which could be used as proof *to another person* of the vote cast" [MG06: 10, italics added for emphasis]. Although McGaley and Gibson do not comment on such nuances, it seems clear that they interpret this recommendation with a teleological approach that permits some means of individual verification only for the voter.

In our opinion, it makes little sense to consider the Council of Europe's 51st recommendation as being only applicable to the voter because the risk that it intends to avoid only exists if the proof of content can be transferred to third parties. Only when the vote's content can be proven to a third party does a voting receipt make voters susceptible of voter coercion or vote buying. When the voting system includes features

[10] Both systems emphasize that e-enabled remote voting systems might always include a non-remote individual verifiability by using voting booths where each voter will receive data about his or her ballot without being submitted to any external pressure. Note, however, that such solutions have to admit a non-remote stage so that individual verifiability and a fully remote procedure will not be feasible. However, the Norwegian project aims to join both features.

[11] Wolter Pieters adds an interesting nuance to coercion resistance systems that would only exist if people were not "able to prove how they voted, *even if they want to*" [Pi06: 2; italics added for emphasis]. Again, if we apply such meaning to the Norwegian case, the first perception is misleading. At a first glance, return codes would not be admitted by Pieters as proper coercion resistant means because they would allow the voter to prove how he or she had voted. The system does not automatically preclude such an option, what it is envisaged by Pieters, but, even if the voter wants to reveal how s/he voted, the system will always render this decision meaningless because the potential coercer will never be sure whether the voter can be trusted.

such as multiple voting options and the primacy of the p-ballot, which deletes the dangers of a voting receipt being transferred to third parties, the fact that the voter is in possession of a proof of content is not important. Such return codes may breach the literal wording of the Council of Europe's 51st recommendation but using a broader legal assessment that includes a teleological approach, one can reasonably conclude that return codes fall well within the boundaries of the recommendation's goal.

6 Concluding Remarks

The Norwegian Internet voting project aims to improve the management of remote voting channels with some new features: a transparent policy that publishes all the relevant documentation, a software independent verification system that includes E2E tools, and voting receipts that intend to provide partial individual verifiability to each voter. These steps will likely become important benchmarks in the provision of Internet voting systems elsewhere.
This paper has focused on the so-called return codes. The discussion is based on whether such components may breach the secrecy of the vote and whether they comply with international standards that prohibit the use of a voting receipt for remote voting channels. The first issue is resolved by mixing return codes with multiple voting so that potential coercers will never know whether the code links to a counted ballot.

The second problem requires the reinterpretation of such standards concerning e-voting. A literal interpretation may lead to the conclusion that any proof of content provided by a remote voting system to the voter is prohibited. However, a teleological method seems more appropriate in order to discover the actual goal of the Council's recommendations. Applying such an approach leads to the conclusion that what is forbidden is the ability to use a voting receipt to prove to third parties the content of the vote, not proof only of value to the voter. If the return codes are meaningless for third parties, as they are in the Norwegian Internet voting system, they can be considered voting receipts while still fully meeting the requirements of international standards like the Council of Europe's *Recommendations on E-voting*.

Bibliography

[Al83] Alexy, R.: Theorie der juristischen Argumentation: die Theorie des rationalen Diskurses als Theorie der juristischen Begründung. Frankfurt am Main, Suhrkamp, 1978 (translation: A Theory of legal argumentation: the theory of rational discourse as theory of legal justification. Oxford, Oxford University Press, 1989)

[Bu11] Bull, C.: Safety first! Verifiability in the e-vote 2011-system. In: E-voting Conference. Oslo, Ministry of Local Government and Regional Development, 2011.*www.regjeringen.no/upload/KRD/Prosjekter/e-valg/e_vote_conference/ ChristianBull.pdf* [November 30th 2011]

[Gj11] Gjøsteen, K.: The mathematics of Internet voting. Oslo, Kommunal- og regionaldepartementet, 2011. *www.regjeringen.no/upload/KRD/Prosjekter/evalg /e_vote_conference/Gjosteen_evalgskonferanse.pdf* [November 10th 2011]

[Gj10] Gjøsteen, K.: Analysis of an Internet voting protocol. In: Cryptology ePrint Archive - Report 2010/380. *eprint.iacr.org/2010/380.pdf* [February 11th 2012]

[Jo09] Jones, D.: Some Problems with End-to-End Voting. In: End-to-End Voting Systems Workshop. Washington D.C., National Institute for Standards and Technology (NIST). *www.divms.uiowa.edu/~jones/voting/E2E2009.pdf* [December 23rd 2011]

[Jo07] Jones, D.: The Impact of Technology on Election Observation. In: VoCom. Portland, VoComp. *www.divms.uiowa.edu/~jones/voting/vocomp07.pdf* [December 23rd 2011]

[Jo04] Jones, D.: The European 2004 Draft E-Voting Standard: Some critical comments. Department of Computer Science / University of Iowa. *www.divms.uiowa.edu/~jones/voting/coe2004.shtml* [February 11th 2012]

[MG06] McGaley, M.; Gibson, J. P.: A Critical Analysis of the Council of Europe Recommendations on e-voting. In: EVT'06. Accurate / Usenix, 2006. *www.usenix.org/events/evt06/tech/full_papers/mcgaley/mcgaley.pdf* [February 11th 2012]

[NS11] Nore, H.; Stenerud, I.: The good, the bad and the terrible of verifiable electronic voting. In: VoteID11 / 3rd International Conference on E-Voting and Identity. Tallin, 2011.

[Os06] OSCE/ODIHR: The Netherlands. Parliamentary Elections 22 November 2006. OSCE/ODIHR Election Assessment Mission Report. Warsaw, OSCE/ODIHR. *www.osce.org/odihr/elections/netherlands/24322* [24th December 2011]

[Pi06] Pieters, W.: "What proof do we prefer? Variants of veriability in voting", Workshop on Electronic Voting and e-Government in the UK, Edinburgh: e-Science Institute, pp. 33-39. *doc.utwente.nl/65114/1/Verifiability.pdf* [February 11th 2012]

[Ri11] Riise, M.: The Norwegian e-Voting Trials Legal Framework, E-Voting Conference. Oslo, Ministry of Local Government and Regional Development, 2011. *www.regjeringen.no/upload/KRD/Prosjekter/e-valg/e_vote_conference/ MarianneRiiseE-voting_conf_11092011.pdf* [February 16th 2012]

[Sm10] Smith, E.: Hemmelige elektroniske valg? In: Lov og Rett, 49(6), pp. 307-323.

[SVK11] Spycher, O.; Volkamer, M.; Koenig, R.: "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting", VoteID11 / 3rd International Conference on E-Voting and Identity. Tallin, 2011. *e-voting.bfh.ch/app/download/ 5022330961/SVK11.pdf?t=1314955570* [February 16th 2012]

[Ve04] Venice Commission: Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe. Strasbourg, European Commision of Democracy Through Law. *www.venice.coe.int/docs/2004/CDL-AD%282004%29012-e.asp* [October 28th 2011]

Session 2

The Technology behind the Norwegian Internet Voting

Cast-as-Intended Verification in Norway

Jordi Puiggalí Allepuz, Sandra Guasch Castelló

Scytl Secure Electronic Voting
08006 Barcelona, Spain
{jordi.puiggali | sandra.guasch}@scytl.com

Abstract: The Norwegian Ministry started an initiative to implement Internet-voting trials during the municipal elections in 2011. One of the security requirements of the chosen e-voting system to not to put any trust in the voting client: a malicious application controlling the voting client should not be able to modify the voting options selected by the voter without being detected. This paper describes the voter verification return-code scheme that was implemented for this project. Furthermore, this paper explains the implementation details of the final solution and the workflow of the system during the different election phases. The aim of this paper is to provide a general overview of the cast-as-intended scheme implemented in eValg2011.

1 Introduction

In August 2008, the Norwegian Ministry started a project whose initial target was to implement remote electronic voting trials in selected municipalities during the municipal elections in 2011. The final objective was to introduce the system throughout the country in subsequent elections.

The eValg2011 voting platform was successfully used in ten municipalities during the municipal and county elections in 2011. Voters in these municipalities had the opportunity to vote on the Internet from their homes. In total, 53,481 votes were cast within an electoral roll of about 165,000 voters (ten municipalities), representing 73% of the advance votes and 16.6% turnout when compared to the federal census. Authorities plan to use the same voting platform in future municipal elections and referendums.

Many of the e-voting system's security requirements [EV09] to be implemented for the eValg2011 project were defined during the bidding phase. Specifically required was the ability to detect potential vote manipulations by a malicious voting client when casting a vote. Therefore, absolute trust in the voting client software was not mandatory.

In remote electronic elections, the voting client software is generally in charge of receiving the voting options chosen by the voter and encrypting them before sending the vote to a server, meaning that voters have to trust that the voting client is not going to change their selections before being encrypted. However, in case the voting client would do it, the probability of being detected is very low. Cast-as-intended verification methods have been designed to prevent such deception: voters do not need to trust the voting

client software to encode the selected voting options properly, since they can audit the process. This has been achieved in the eValg2011 project by using a cast-as-intended verification scheme based on using return codes.

The aim of this paper is not to describe the full cryptographic voting scheme implemented in the eValg2011 voting system, only the cast-as-intended verification scheme implemented in the system. This paper starts by describing the differences between the initial protocol proposed by Puiggali-Guasch [PG11] and the final protocol implemented in the eValg2011 voting system. It also describes how the design of some parts of the verification mechanisms (mainly the return codes) evolved during the project until reaching the final design used in the 2011 elections.

This paper is organized as follows: In section 2, the existing proposals for cast-as-intended verification are presented. Section 3 briefly presents the changes made to the original scheme for the eValg2011 project. Section 4 shows an overview of the voting system as seen by the voter. Section 5 presents the building blocks of the underlying protocol designed for the cast-as-intended verification mechanism. Section 6 explains the election configuration process. In section 7, the voting phase is presented. Section 8 shows the SMS formats used to provide the voters values for the cast-as-intended verification, and the paper concludes with some final remarks in section 9.

2 Cast-as-Intended in Remote Voting

There are mainly two different approaches for providing cast-as-intended verification in remote voting: methods based on challenging the voting client and methods based on using return codes.

In methods that challenge the voting client, such as the one implemented in the Helios system [Ad08], the voting application commits first to the encrypted vote before it is cast and asks the voter later if she wants to verify the correct encryption of her choices before casting the vote. The commitment is usually the hash value of the encrypted vote that is shown at the top of the voter screen in a user-friendly format (e.g., base64 text encoding). If the voter decides to challenge the system, the voting application discloses the encryption parameters. The voter can then reproduce the same encryption operation of her voting options to verify if the resulting ciphertext has the same hash value as the one committed by the voting application. To perform the encryption and verification of the commitment, the voter can use a tool provided by any independent, trusted party, or the voter can just send the commitment and disclosed information to an external auditor along with the selected voting options. Each time the voter challenges the system, the encrypted vote is discarded and the voter is allowed to change the intent and cast a new one. The challenging process is shown each time before casting a vote. Therefore, the voter can challenge the system as many times as requested.

The systems based on return codes require sending a special voting card to voters in advance of the election. This card contains a list of short codes (e.g., four digit numbers) correlated to the possible voting options. These voting cards are unique and different for each voter and therefore, voters never have the same codes for their voting options. The verification process is usually implemented after casting the vote. In this case, the voting server usually performs a cryptographic operation over the cast vote that generates a code that is returned to the voter. The voter then checks in the voting card if the received code has the same value as the code present on the card for her selected choice. Within the return codes-based systems, it is possible to distinguish between two systems, one that includes an additional code used to cast the vote on the same voting card [St07], [MSP09], [MMP02], [Ch01], [Ce02], [VZ05], [HS07], [CCE11] (known as pollsterless or pre-encrypted ballot systems) and one that does not include this code [PG11], [Li11].

The eValg2011 voting system was based on the latter, and, more specifically, it is a variation of the Puiggali-Guasch proposed scheme.

3 Changes Made Over the Original Scheme

The modifications made to the Puiggali-Guasch scheme to develop the eValg2011 project were mainly focused on moving cryptographic processes implemented in the voting client to the voting servers.

In the original Puiggali-Guasch proposal, the voting client implements a set of cryptographic operations over the voting options to generate a special ciphertext with deterministic properties, which allow for the generation of the return codes of the selected voting options contained in the encrypted vote. This ciphertext is sent to the voting server along with the encrypted vote and a proof of content equivalence between this special ciphertext and the encrypted vote. A set of cryptographic operations are implemented by the voting server and another independent server (known as the return code generator) for generating the return codes.

In the eValg2011 protocol, the voting client does not generate any special ciphertext for the return codes; it simply encrypts and casts the vote. The special ciphertext with deterministic properties is generated in the voting server by executing a set of cryptographic processes over the encrypted vote cast by the voter. This ciphertext is then forwarded to the return code generator server which applies a second set of cryptographic operations for generating the return codes. This change implied a complete re-design of the cryptographic operations and content equivalence proofs implemented by the scheme. The re-design was lead by Kristian Gjøsteen, and its security is further discussed in [Gj10].

There are several advantages that this re-imagined scheme offers:

- A reduction of the cryptographic operations implemented in the voting client: the voting client does not generate the special ciphertext nor the proof of content equivalence of the original scheme; it only encrypts the vote.
- The improvement in usability of the voting process: the voter iss not required to introduce any voting card identifier for verifying the return codes (as required in the original scheme).

However, these advantages have some side effects:

- Special measures must be implemented to prevent any collusion between the voting server and the return code generator, otherwise both servers could compromise the voter privacy.
- The number of cryptographic operations performed in the servers increases substantially, since the operations initially executed in the voting terminal for generating the special ciphertext, must be now executed by the servers.

It is of special importance to mention that one of the security requirements under which both schemes were designed was that one single component or participant in the voting system (voting client, voting servers, etc.) should not be able to cheat in the election process without being detected: i.e., one single component should not be able to act in a different way that what is described in the protocol in order to break voter privacy or affect the integrity of the election. The way this is fulfilled is further analyzed throughout the following sections, as well as in [SVK11].

4 Overview of the Voting Process

In order to better understand the return code scheme implemented for the eValg2011 project, we will present a brief overview of the voting process as seen by the voter:

Before or during the voting phase, the voter receives a voting card containing the return code values assigned to each possible voting choice, which will be used to verify that the voter's selections have been correctly received by the voting server.

During the voting process, the voter is authenticated by the system. Once the eligibility of the voter has been verified, the voter receives her credentials, which will be used to digitally sign her vote. The voter uses a voting Java applet to select her choices. Once the voter has finished making her selection, the completed ballot is encrypted using an election public key and digitally signed using the voter credentials. The vote is then sent to a voting service (known as the vote collector server or VCS), where it is stored in the electronic ballot box. The voting service forwards the vote to a validation service (called the return code generator or RCG), where the return codes representing the selected voting options are generated and then sent to the voter via SMS message. The voter uses the voting card to verify that the return codes correspond to her completed ballot.

The cast-as-intended scheme can be split in two levels: the core level, where the cryptographic operations are implemented, and the presentation level, which manages how the results of the cryptographic operations are shown to the voter.

In the core level, each voting option is linked to a unique return code value. However, at the presentation level, unique return code values could be linked to a new, shared return code in order to improve the usability of the voter verification process. For instance, the presentation level could link the unique return code of a candidate obtained from the core level to a generic return code signifying the position of the candidate inside the party list. Therefore, the number of return codes managed by the voter is drastically reduced: all the candidates having the same position in different party lists would have the same position return code.

Currently, the eValg2011 system can generate three different types of return codes for voters at the presentation level:

- Unique return codes for each voting choice: they are a direct representation of each return code generated at the core level.
- Position return codes related to the position of voting options within a list of options: in this case, core level return codes of different candidates will share the same position return code if they are located in the same position on a selection list (e.g., the first candidates of different party lists will share the same return code representing the first position within a list). These position return codes are usually combined with unique return codes identifying the list that the candidate position is related to (i.e., every candidate is represented by a tuple composed by a unique party return code and a position return code).
- No return codes, but information related to the number of selections made within a list: this approach is used when the voter makes selections within different lists. In this case, the presentation layer combines the use of a unique return code representing the list (e.g., a party return code) with the number of selections made within the list (i.e., an explicit message documenting the number of selections made instead of candidate or position return codes). This is the specific scheme used in the municipal and county elections conducted in 2011 as part of the eValg2011 project.

All these return code representation options are configurable at the voting system and have been tested in different trials before the 2011 municipal and county elections.

For simplicity, we will describe the system using the unique return code representation used at the core level as reference. The different return code representations at presentation level are discussed in the sections related to the generation of the voting cards and return codes sent by SMS. The usability and security implications of the approach of working with each return code representation at presentation level will be discussed in Section 8.

5 Building Blocks

The return code generation scheme is composed of the following building blocks:

Underlying Cryptosystem: The vote is encrypted using a probabilistic encryption algorithm suitable for use with zero-knowledge proof schemes [MOV96]. In this specific implementation, the encryption algorithm is ElGamal [El84]. The election cryptosystem is composed of three public parameters: *p*, *q*, *g,* with *p=2q+1*; an election public key h_e; and an election private key x_e defined in the ElGamal scheme.

We denote a vote composed of several encrypted voting options as $v_{opt_i} = (a_i, b_i) = (g^{r_i}, v_i \cdot h_e^{r_i})$, where the encryption exponents r_i are chosen as random values from Z_q, the operations are done modulo *p,* and each value v_i represents a voting option.

Besides the election keys, two ElGamal key pairs are used for the return code generation process: one for the VCS (h_{vcs} , x_{vcs}) and one for the RCG (h_{rcg} , x_{rcg}). Both key pairs are defined by the same parameters (*p*, *q*, *g)* of the ElGamal scheme as the election key pair For the purpose of the protocol, these keys have the following mathematical relationship: $x_{rcg} - x_{vcs} \equiv x_e \pmod{p}$.

The security threats and countermeasures regarding this key relationship are discussed further in [Gj10].

Voter Secret Parameter: In order to be able to generate different return codes for different voters, the voting options cast by a voter are raised to a value *s* that is different for each voter (voter secret parameter) in the VCS, in order to get a *personalized,* random encryption for each voter. These values are used during the configuration and the voting phase. Therefore, they cannot be generated on-the-fly and must be stored in a secure way. A hardware security module (HSM) could be use to securely store this information. However, there may be millions of values to store (one per voter), which could be a problem. To solve this, only a private key is securely stored and *s* values are derived in the VCS using this cryptographic key and a pseudorandom function. Therefore, the output of this pseudorandom function will be random for someone without the cryptographic key.

In this specific implementation, the pseudorandom function used to generate the voter secret parameter *s* is a symmetric encryption algorithm (AES - CBC mode [FP01]). Therefore, the voter secret parameter *s* is generated as the AES encryption of a random voter identifier in the election (*voterID*) using a secret key stored in the VCS, K_{vcs}. The *voter ID* must be padded or transformed in such a way that it is long enough to generate a 2048-bit value for *s*. It is important to have a large value for *s*, since it is in charge of protecting the secrecy of the vote in several specific steps of the process.

Zero-knowledge Proofs: Return code values are generated with the collaboration between the VCS and the RCG, in the sense that the first makes some partial calculations and sends them to the second, which generates the final values. This way, the knowledge needed to generate valid return codes is split into two independent components of the voting system, so that both have to be compromised in order to cheat the voters. However, each component has to prove to the other one that it is following the protocol properly. If not, one component would be able to cheat in the election. For example, VCS could use the vote of one voter to make the RCG generate the return code values for another voter. Therefore, return codes corresponding to the selections made by the first voter are sent to the second one, invalidating the first voter's privacy. Non-Interactive zero-knowledge proofs (like Schnorr proofs in [Sc91]) are used by the VCS to demonstrate to the RCG that the partial calculations actually belong to a specific valid vote.

6 Election Configuration Process

The main objectives of the election configuration process are to create the keys used for computing the return codes and to generate the voting cards used by the voters to verify the correct representation of their voting options inside the encrypted vote.

6.1 Generation of Election Keys

The eValg2011 voting system mainly uses two different sets of keys for implementing the cast-as-intended verification scheme:

- *Asymmetric keys*: used to protect the privacy of the vote.
- *Symmetric keys*: used to generate a deterministic value of the encrypted vote contents in order to calculate return codes.

Asymmetric Key Generation: As presented in Section 5, the eValg2011 solution relies on the following relation between the x_{vcs} private key of the VCS, the x_{rcg} private key of the RCG, and the x_e election private key $x_{rcg} - x_{vcs} \equiv x_e \pmod{p}$. This relationship is required for retrieving ciphertexts with deterministic properties from the encrypted votes.

The VCS and RCG keys are generated in two different, isolated environments to prevent both keys from being used to reconstruct the election private key. We will identify these environments as voting card generation (VCG) modules. During the key generation process, VCS and RCG private keys are split into shares (using a Shamir secret sharing scheme [Sh79]) that are distributed among the members of an electoral board. The shares are stored using PIN protected smartcards owned by the members. Since VCS and RCG keys are generated in two different environments, electoral board members participate in two different processes. Finally, each member will hold two shares, each one from a different private key (x_{rcg}, x_{vcs}). The election's private key is never generated, since it

can be reconstructed at the end of the election from the shares owned by the electoral board members. Only the public key is generated, using the public keys of the VCS and RCG. The private keys (x_{rcg}, x_{vcs}) are also uploaded to the corresponding servers VCS and RCG in a secure way (encrypted).

Symmetric Key Generation: The VCS and RCG also require symmetric secret keys for implementing the cryptographic operations to generate a deterministic value related to the encrypted vote contents (i.e., the return code sent to the voter). These keys (K_{vcs}, K_{RCG}) are generated using a secure random number generator. They are uploaded to the corresponding servers in a secure way (encrypted).

6.2 Generation of Voting Cards

According to the different return code representation options at the presentation level explained in Section 4, the voting cards may have different formats: they may have unique return code values for each option and/or return code values representing positions. For the sake of simplicity, we will explain how the voting cards are generated when position return codes are used to represent the candidates from party lists, and unique return codes are used to represent each party list. This is the most complete case of return code representation options. The municipal and county election used a simplified presentation with only unique return codes per party lists.

The voting card is a paper sheet containing a unique return code for each party list and for each position on the party list. Although the scheme supports return codes per candidate, candidates are represented by their position on the party list in order to make the voting card management and the return code comparison process (for voter verification) more usable for the voter. Certain Norwegian elections could have 25 parties with, in some cases, 99 candidates. If individual return codes per candidate are used, the amount of codes on the voting cards could be approximately 2,500 codes (25+(99*25)). Using position codes, the voting card will only need 124 codes (25+99). Other return code representation options were also implemented in the different elections and pilots carried out. All of them, as well as their risks and impact, are discussed in Section 8 of this paper.

Voting cards are used to verify that the voter's intent was properly recorded (cast-as–intended verification) by the ballot box located in the VCS. To this end, after the voter casts a vote, the RCG calculates (in collaboration with the VCS) and returns the return codes of the party and the candidate's position in this party for each selected candidate. Since these values are obtained from operations using the encrypted vote, voters can verify if their cast votes contain their selected voting options by comparing the return codes returned by the RCG with the ones available on the voting card for the same selected voting options. The fact that the voting card is only available on paper and is only known by the voter makes it impossible for a compromised component of the voting platform (the voting client, the RCG, etc.) to subvert the cast-as-intended verification method, by profiting from the knowledge of the return code values. This

could allow the component to change the voting options cast by the voter and send the return codes corresponding to the original selections. These return codes are sent to the voter through a different channel (SMS) than the one used for casting the votes.
An example of how this verification of parties and positions works is shown in the Figure 1.

Fig. 1: Cast-as-intended verification with voting cards

Therefore, the voting card contains two sets of return codes:

- Party return codes
- Position return codes

Due to usability and SMS message length constraints, the party and position return codes sent via SMS are limited to 4 numerical characters (original codes obtained by the return code generator have 256 bits length, equivalent to 43 characters in base64 representation). This could generate collision issues between two different options if the original codes are only truncated (i.e., two different choices could end up with the same code on the voting card). Therefore, these SMS codes are generated in advance (controlling possible collisions) and mapped to the original codes in a secure way by combining a hash and encryption function. This mapping database is stored in the RCG during the election configuration phase.

A multi-party generation process is used to calculate the return code data during the election configuration phase. To this end, the two different and isolated VCG environments (VCG1 and VCG2 modules) are used to reproduce the same *deterministic* transformation of the votes that will be carried out by the VCS and RCG during the voting process: VCG1 implements the VCS transformation, and VCG2 implements the RCG transformation and links the result to the return codes that will be sent to the voter. This separation of duties prevents both VCG1 and VCG2 from correlating the generated return codes with the identity of the voters they belong to (VCG1 knows the voter identities; VCG2 knows the return code values). Therefore, an attacker controlling only one of these modules cannot influence the election results without being noticed.

The voting card and return code generation process done during the election configuration phase is divided into the following steps:

Calculation of Initial Candidate and Party (long) Codes: These are the codes obtained after applying the VCS and RCG cryptographic operations over each individual ciphertext that composes the encrypted vote cast by the voter (containing the code of the party list or candidate). This process is split between the VCG environments.

In a first step, the VCG1 generates random voter identifiers *voterID* and computes for each one a partial calculation of party and candidate codes as:
$s = AES_{K_{vcs}}(voterID')$, $P_i' = P_i^s \bmod p$, $C_i' = C_i^s \bmod p$

These partial calculations of party and candidate codes and related random voter identifiers are passed to the VCG2 module using an offline (air-gapped) channel.

Secondly, VCG2 calculates the final values of the party and candidate codes using the partial calculation from VCG1: P_i' and C_i', an HMAC function, a secret key K_{rcg}, and the random voter identifier *voterID*.
$PartyCode_i = HMAC(P_i' \,||\, voterID,\ K_{rcg}),\ CandCode_i = HMAC(C_i' \,||\, voterID,\ K_{rcg})$

Calculation of Party and Position (short) Return Codes: These are the short codes representing the parties and positions of candidates on party lists, which are printed in the voting cards. Since the SMS position and party return code values will be different for each voter, they are calculated by VCG2 follows:
$PartyReturnCode_i = HMAC(voterID \,||\, party_i,\ K_{rcg})$
$PosReturnCode_i = HMAC(voterID \,||\, position_i, K_{rcg})$,
where $party_i$ and $position_i$ are constant numeric values assigned to parties and positions.

Mapping Party and Candidate (long) Codes with Party and Position Return (short) Codes: VCG2 hashes each possible party or candidate code and stores it in the table connected to the party or position return code corresponding to it:
$H(PartyCode_i) \leftrightarrow PartyReturnCode_i$
$H(CandCode_i) \leftrightarrow PosReturnCode_i$

This table is randomized and finally deployed in the RCG, so that it is able to correlatevthe party and candidate codes with the party and position return codes during the voting process (without knowing the connection to the original party and candidate names). As we mentioned before, the return codes sent to the voter shall not be known by any component of the platform.
Otherwise, the voter selections could be changed and the attacker could send the return codes corresponding to the original vote to cheat the voter.

Therefore, in order to prevent the RCG from knowing the party and position return code values in advance, each return code is encrypted using the corresponding party or candidate code (which has to be generated in collaboration with the VCS from a valid vote) as a symmetric key ($AES_{PartyCodei}(PartyReturnCode_i)$ / $AES_{CandCodei}(PosReturnCode_i)$).

Printing and Assigning Voting Cards to Voters: Finally, party and position return codes and random voter identifiers (*voterID)* are given to the printing service for printing the voting cards. Once printed and in an envelope, each *voterID* is assigned to a valid voter identity and an envelope containing the voting card is sent to the voter address. The link between the *voterID* and the voter identity is kept on the electoral roll to allow the VCS to retrieve the correct *voterID* value during the voting process.

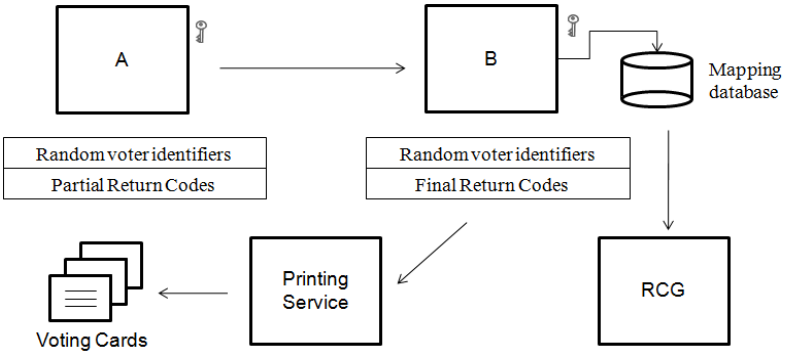


Fig. 2: Return code information generation during the configuration phase

A diagram of the return code information generated during the election configuration phase is shown in Figure 2 (modules A and B in the picture represent the VCG1 and VCG2 environments).

7 Voting Phase

As already mentioned, during the voting phase the return code generation process is split into two processes performed by two independent modules, the VCS and the RCG. This prevents a malicious single entity from cheating voters without being detected.

During this phase, the VCS executes a first set of cryptographic operations over the encrypted, cast vote, which are then forwarded to the RCG. The RCG executes a second set of operations to generate the final return code values. The VCS and RCG keys generated in the election configuration phase are used during the voting phase to perform such operations. In order to ensure that the calculations in the VCS are fair (e.g., to prevent the VCS from trying to make the RCG return codes from another vote or voter), several zero-knowledge proofs (ZKPs) are generated, relating the partial calculations from the VCS to a specific voter.

Once completed, the following steps are carried out:

Vote Encryption and Casting: The voting options chosen by the voter are individually encrypted using the election public key and sent to the VCS: $v_{opt_i} = (a_i, b_i) = (g^{r_i}, v_i \cdot h_e^{r_i})$

Vote Re-encryption and Partial Decryption: VCS applies some sort of re-encryption of the voting options using a voter-secret parameter *s*. This re-encryption is used to get a *personalized,* random encryption for each voter, which will be used to generate the return codes. The *s* parameter is calculated using the random voter identifier and the secret key K_{vcs} ($s = AES_{K_{vcs}}(voterID')$). The re-encryption consists of raising the encrypted voting options to this *s* value: $v_{opt_i}' = (a_i', b_i') = (a_i^s, b_i^s)$

After re-encrypting the voting options, the VCS performs a partial decryption of the result: $b_i'' = b_i' \cdot a_i'^{x_{vcs}}$

Finally, the VCS generates non-interactive ZKPs of the calculations made on the cast vote. These ZKPs allow the RCG to validate the correctness of such operations. The VCS generates two sets of ZKPs to prove the validity of the values:

- A proof that demonstrates that the VCS identified and used the correct voter secret parameter *s* to re-encrypt the vote (i.e., that is not using the parameter *s* of another voter)
- A proof demonstrating that the VCS identified and used its ElGamal private key x_{vcs} for partially decrypting the re-encrypted vote.

The encrypted vote (as originally cast by the voter) and the result of the VCS and ZKPs are sent to the RCG.

Vote Partial Decryption and Generation of Return Codes: The RCG verifies the ZKPs in order to ensure that the VCS calculations are correct and done over a specific vote. If they are correct, it partially decrypts the vote (already partially decrypted by the VCS) using its private key: $b_i'' \cdot a_i'^{-x_{rcg}} = b_i^s \cdot a_i^{s \cdot x_{vcs}} \cdot a_i^{s \cdot (-x_{rcg})} = (b_i \cdot a_i^{x_e})^s = v_i^s$

and retrieves the party and candidate codes related to the contents:
$\{Party/Cand\}Code_i = HMAC(v_i^s \,||\, voterID,\ K_{rcg})$

The RCG uses a hash of these codes to retrieve the related return codes from the database:
$H(PartyCode_i) : AES_{PartyCodei}(PartyReturnCode_i)$
$H(CandCode_i) : AES_{CandCodei}(PosReturnCode_i)$

In case the hash of the code is not found in the database, the RCG assumes that the vote which was cast does not contain a valid value. If so, an error is reported to the voter and the vote is rejected. This mechanism prevents the acceptance of votes containing invalid options. The return codes are formatted and sent to the mobile phone of the voter via an SMS gateway.

The process is shown in Figure 3:

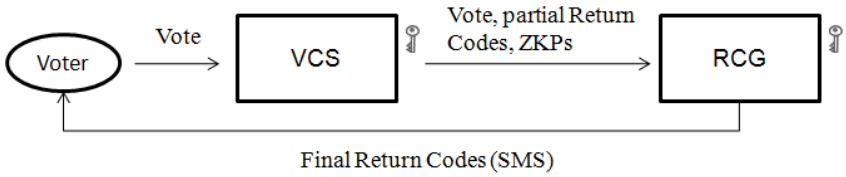


Fig. 3: Return code generation during the voting phase

8 SMS Format

As mentioned before, using SMS messages introduces length and usability constraints for verifying the vote. This has a direct impact in the soundness of the verification process. The format and contents of the SMS messages have been reviewed and tested in several pilots to achieve a good balance between usability and verifiability soundness. Two different SMS formats based on the different return code representation options given at the presentation level, are used: position return codes and the number of candidate selections. In both cases, party return codes are always reported.

SMS with Candidate Position Return Codes: In this case, the message initially contains the party return code, followed by the return codes of the selected candidate's position (if any) for that party.

Figure 4 shows a sample SMS sent to a voter:

You cast a vote for party $PartyReturnCode_1$ candidate positions $PosReturnCode_1$, $PosReturnCode_{2...}$

Fig. 4: SMS format with Position Return codes

SMS with the Number of Candidate Selections: This is the approach used in the last election carried out using this voting platform. In this case, the SMS message only contains the party return code value and a text mentioning the number of selected candidates for that particular party (if any).

Figure 5 shows a sample SMS sent to a voter.

You selected 3 candidates from party $PartyReturnCode_1$

Fig. 5: SMS format with position Return codes

Soundness of the Verification Process: Different return code representation options have a significant impact on the soundness of cast-as-intended verification. When only the party return code and the number of candidates selected are sent to the voter, she cannot verify if the candidate options registered in the voting platform are actually what she selected. She only knows that the number of selections is correct but not if the actual candidate from the party was cast as intended. When party and position return codes are used, the verification process could be subverted if the candidates are shown to the voter in a different position than the official one. Therefore, it is clear that there is a significant tradeoff between usability and soundness. The government's decision to use these representations was made after evaluating these risks and finding out that they did not apply to voters who only select party lists (about 98% of the voters).

9 Final Remarks

One of the aspects highlighted by this paper is how usability influenced several implementation details of the proposal. Initially, usability influenced the decision of to re-design the original cryptographic scheme. This made the system less dependent on the resources available from the voter's computer (enhancing the response time of the voting process). Usability aspects were also of paramount importance for designing the format and contents of the voting cards and SMS messages. In this case, the verification soundness was reduced to achieve a better voter understanding of the verification process (e.g., reporting the number of candidates selected in a party instead of which candidates or candidate positions). Finally, the cast-as-intended method described here protects the integrity of the vote from malicious software installed in the voting terminal. However, it does not protect the voter from other malware attacks, such as capturing voter credentials. This could be considered a serious risk in Norway since voters are allowed to cast multiple ballots. However, the current use of an authentication method based on digital certificates and one-time passwords mitigates this type of attack.

Bibliography

[Ad08] Adida, B. 2008. "Helios: web-based open-audit voting", in Proceedings of the 17th Conference on Security Symposium (San Jose, CA, July 28 - August 01, 2008). USENIX Association, Berkeley, CA, 335-348.

[CCE11] Chaum D., Clark J, Essex A, Rivest R, Sherman A, Vora P., Zagorski F. "Remotegrity". Crypto 2011 rump session. August 16, 2011.

[Ce02] CESG (Communications and Electronic Security Group). "E-voting security study", annex C. 2002. Available at: http://www.edemocracy.gov.uk/library/papers/study.pdf 2002

[Ch01] Chaum D. "SureVote: Technical Overview", Proceedings of the Workshop on Trustworthy Elections (WOTE '01), presentation slides, August 2001.

[El84] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Proc. of CRYPTO 84, pp 10-18.

[EV09] e-Vote 2011 Security Objectives. 2009. Online: http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/tekniskdok/Security_Objectives_v2.pdf

[FP01] FIPS PUBS 197: Advanced Encryption Standard (AES). 2001. Online: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[Gj10] Gjøsteen, K. 2010. "Analysis of an internet voting protocol". Cryptology ePrint Archive, Report 2010/380. Online: http://eprint.iacr.org/2010/380

[HS07] Helbach, J., Schwenk, J. "Secure Internet Voting with Code Sheets". E-Voting and Identity, First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers. Springer 2007, ISBN 978-3-540-77492-1, pp.166-177.

[Li11] Lipmaa, H. "Two Simple Code-Verification Voting Protocols". IACR Cryptology ePrint Archive 2011: 317 (2011).

[MMP02] Malkhi D. Margo O., and Pavlov E. "E-voting without 'cryptography'". In Matt Blaze, editor, Financial Cryptography, 6th International Conference, FC 2002, Revised Papers, volume 2357 of Lecture Notes in Computer Science, pages 1–15, Southampton, Bermuda, 2003. International Financial Cryptography Association, Springer.

[MOV96] A. Menezes, P. van Oorschot, and S. Vanstone. "Handbook of Applied Cryptography" CRC Press, 1996.

[MSP09] Morales-Rocha, V., Soriano, M. and Puiggalí, J. "New voter verification scheme using pre-encrypted ballots". Comput. Commun. 32, 7-10 (May 2009), 1219-1227.

[PG11] Puiggalí, J. Guasch, S. "Internet Voting System with Cast-as-intended Verification". VoteID 2011. Tallinn, Estonia, September 2011.

[Sc91] Schnorr C. "Efficient Signature Generation by Smart Cards". Journal of Cryptology vol. 4 (3) 1991.

[Sh79] Shamir A. 1979. How to share a secret. Commun. ACM 22, 11 (November 1979), 612-613.

[St07] Storer, T. "Practical Pollsterless Remote Electronic Voting". Thesis, 2007.

[SVK11] O. Spycher, M. Volkamer, R. Koenig. "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting". VoteID'11, 3rd International Conference on E-Voting and Identity. Tallin, Estonia, 2011.

[VZ05] Voutsis, N., Zimmermann, F. "Anonymous code lists for secure electronic voting over insecure mobile channel"s. Proceedings of Euro mGov 2005, Sussex University, Brighton, U.K., 10-12 July 2005.

Random Block Verification: Improving the Norwegian Electoral Mix-Net

Denise Demirel[1], Hugo Jonker[2], and Melanie Volkamer[1,3]

[1]Security, Usability and Society group,
CASED, Darmstadt, Germany
ddemirel@cdc.informatik.tu-darmstadt.de

[2]Security and Trust of Software Systems group,
University of Luxembourg, Luxemburg
hugo.jonker@uni.lu

[3]Department of Computer Science,
Technical University Darmstadt
Darmstadt, Germany
melanie.volkamer@cased.de

Abstract: The VALG project is introducing e-voting to municipal and county elections to Norway. Part of the e-voting system is a mix-net along the lines of Puiggalí et al. - a mix-net which can be efficiently verified by combining the benefits of optimistic mixing and randomized partial checking. This paper investigates their mix-net and proposes a verification method which improves both efficiency and privacy compared to Puiggalí et al.

1 Introduction

To ensure anonymity, e-voting systems need to incorporate a mechanism to break the link between the voter and his or her cast vote. One popular method is the use of mix-nets [Cha81], which shuffle the list of encrypted votes while changing the appearance of the ciphertexts and keeping the used permutation secret. To reduce the trust assumption, universally verifiable mix-nets have been developed [SK95, DK00, Wik09, Neff01, Gro10]. Efficiency is a prime concern when voting, To be usable in practice, a mix-net should be able to mix all votes and prove correctness within a few hours after the polling stations have closed. Attempts at efficiency improvement did not raise the bar sufficiently for such a demanding task. Two separate directions in verification sought to address this: optimistic mixing (OM, [GZB02]) and randomized partial checking (RPC, [JJR02]).

Intuitively, OM is able to accelerate the verification process by proving correct mixing for the whole group of inputs: the mix proves that the product of the input ciphertexts is equal to the product of the output ciphertexts (see Figure 1a). While more efficient (only one proof is needed instead of one per input), some fraud may be not detected (intuitively, $4 \times 6 = 3 \times 8$).

The proposal by Golle et al. [GZB02] uses double encryption and a cryptographic checksum to prevent this attack; however, Wikström identified [Wik03] multiple fatal flaws in their particular design. Another optimistic approach by Boneh and Golle, proof of subproduct (PoS, [BG02]), is slightly faster as it does not use a cryptographic checksum or double encryption.

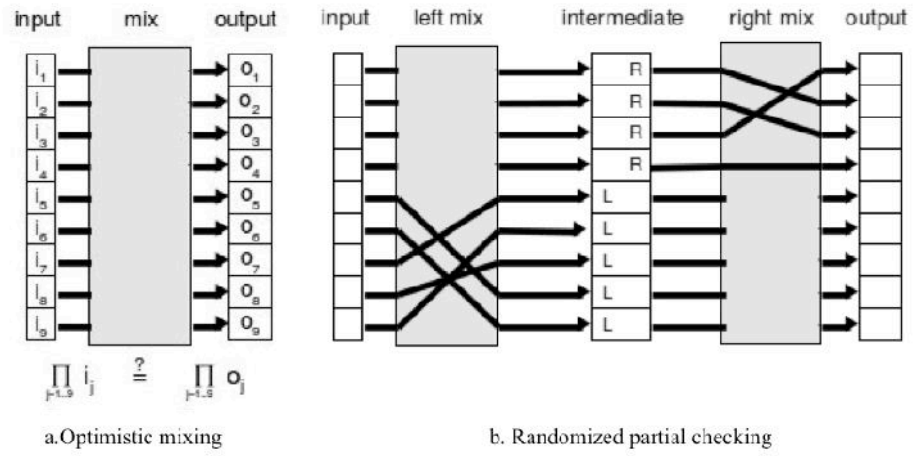


Fig. 1: Two approaches to trading verification for efficiency in mix nets

A drawback of this approach is that the verification only guarantees almost entirely correct mixing. Boneh et al. recommend the use of a slower verification protocol in parallel to guarantee correctness.

RPC lets each mix-node first produce an intermediate shuffle, and then shuffle again to produce the final result. For each element of the intermediate result, a coin is flipped to reveal the link to either its corresponding input (heads) or output (tails) element (see Figure 1b). This approach doesn't require any proof (just revealing half the re-randomization values used), but there's a 50% chance per element for the mix to cheat undetected.

Puiggalí et al. combined the advantages of OM and RPC to arrive at a mix-net design that improves upon privacy and verifiability while retaining efficiency. Their work was incorporated into the Norwegian Evote Project[1] and used for a limited number of municipality elections in Norway. In the recent past, advances have been made in efficient, provably-secure mixing (e.g., [Wik09,Gro10,TW10]). However, these approaches do not align with the current Norwegian implementation. Our goal is to propose an improved verification approach that remains close to the Norwegian design so that the current implementation can be easily updated.

Contribution: The contribution of this paper is twofold: First, this paper identifies several areas for improvement (including a privacy weakness) in the scheme proposed by Puiggalí et al. These improvements are incorporated into *random block verification*

[1] http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/about-the-e-vote-project.html

(RBV), a scheme which is more efficient, more secure, and more precisely detailed. The architecture of RBV remains sufficiently close to the scheme by Puiggalí et al. to allow for easy adoption into the Norwegian system. Second, we analyse the verifiability, privacy, and efficiency of RBV and compare these properties to properties of other mix-nets that offer a trade-off between verifiability and efficiency.

Structure of the paper: The rest of this paper is structured as follows: we first discuss ElGamal mix-nets (Section 2). As this work improves upon the contributions of Puiggalí et al, their research is discussed in more detail (Section 3). Possible improvements to the verification process are discussed in Section 3.1, all of which are implemented by the new verification process detailed in Section 4. Correctness, privacy, and efficiency of the newly proposed verification process are determined in Section 5 and compared to other mix-nets that trade privacy for efficiency. This is followed by conclusions and future work in Section 6.

2 Re-encryption Mix-Nets with Exponential ElGamal

We assume that votes are encrypted using exponential ElGamal and stored on a web bulletin board (BB) where some connection between each encrypted vote and the corresponding voter exist. Exponential ElGamal is a randomized public-key encryption scheme with homomorphic properties introduced in [Elga85]. Consider two large primes p and q, where $q \mid p - 1$. G_q is a q-order subgroup of $\mathbf{Z}_p^*$ and g is a generator of G_q. The secret key $x \in Z_q$ is generated and the corresponding public key is (g,y) with $y=g^x$. A plaintext s (or here a vote) is encrypted in the following way: $Enc_y(s,r1) = (g^{r1}, g^s y^{r1}) = (\alpha, \beta)$ with random value $r1 \in G_q$.

To ensure anonymity, the votes are processed by a re-encryption mix-net. The output of this mix-net is a set of anonymized, re-encrypted votes that can then be decrypted and counted. A re-encryption mix-net with m mix-nodes works as follows: The first mix-node loads all encrypted votes (while removing any possible link to the voter-like signatures) published on the BB as input. Every input ciphertext is re-encrypted by multiplying the ciphertext with an encryption of 1: for $r2 \in G_q$, $ReEnc_y((\alpha, \beta), r2) = (\alpha\, g^{r2}, \beta\, y^{r2}) = (g^{r1} g^{r2}, g^s y^{r1} y^{r2}) = (g^{r1+r2}, g^s y^{r1+r2}) = (\alpha', \beta')$. (Note that while the plaintext remains unchanged, the ciphertext is completely altered.)

Next, the re-encrypted ciphertexts are shuffled with a random permutation π, and the resulting output ciphertexts are published on the BB. Afterwards, the second mix-node loads the output ciphertexts from the first one published on the BB and re-encrypts and shuffles them, as well. This process is repeated until the last one publishes its output ciphertexts on the BB. These are the ciphertexts which are decrypted and counted. Privacy is ensured if at least one mix-node is honest and keeps the permutation secret. In order to ensure that mix-nodes cannot cheat by replacing encrypted votes with new ones, verifiability needs to be implemented, ideally without decreasing the level of privacy.

3 Norwegian Mix-Net by Puiggalí et al.

In [AC10], Puiggalí et al. describe an approach to verify a re-encryption mix-net (with exponential ElGamal) that combines the idea of optimistic mixing and RPC. This verification is executed after the last mix-node has published its output on the bulletin board. The analysis of the Norwegian election system [Gjo10] treated this mix-net as a solid building block. Nevertheless, there is room for improvement - in particular, the verification efficiency of the mix-net can be improved. Below, is a description of the verification process along with several points highlighting where improvements can be made.

The Puiggalí et al. verification process operates as follows:

1. An independent verifier provides a random permutation (the challenge) of all input votes of the first mix-node.
2. To verify, the list of votes is divided into $l = \sqrt[m]{n}$ equally-sized blocks, for *m* mix-nodes and *n* input ciphertexts (i.e., votes). Since *l* is well-defined, this can be executed by either the independent verifier, the BB, or the mix-node.
3. For every input block, the first mix-node identifies the corresponding output block. Moreover, for every block, the mix-node publishes the product of the ciphertexts in that block. Finally, the mix-node publishes a zero-knowledge proof (e.g. using the Chaum-Pedersen protocol [CP93] or Schorr's signature scheme [Sch91]) to prove that the ciphertext product of the input block is equal to that of the corresponding output block.
4. The verifier checks the proofs of the first mix-node.
5. This process continues for each mix-node, where the assignment of nodes to blocks depends on the previous node's assignment - thus ensuring an equal distribution of input ciphertexts over all blocks.

Regarding privacy, Puiggalí et al. state that every output block of the last mix-node is composed of at least one ciphertext of every input block of the first mix-node. Regarding correctness, the authors determine that the probability of detecting two modified votes is $p = 1 - \frac{l-1}{n-1}$ for block size *l* and *n* ciphertexts. Note that any manipulation would remain undetected if a malicious mix-node changes two votes without changing the product of the two ($1 \times 1 = \frac{1}{2} \times 2$) and then assigning them to the same block.

3.1 Remarks

Some remarks to this approach are discussed below. Corresponding improvements are sketched in this section and worked out in Section 4.

Inefficient zero-knowledge proofs. In [AC10], the correct processing of each block is proven with computationally costly zero-knowledge proofs. A more efficient solution is to publish the sum of the random values used for the re-encryption per block. As this does not reveal anything but random noise, this value can serve as a zero-knowledge proof. This is very efficient (as it does not require any zero-knowledge proof). However, proving that this does not reveal any usable information whatsoever in a mathematically rigid fashion is an open question. Therefore, an alternative, while work on this proof continues, is to use efficient zero-knowledge proofs as those from [JJ99]. With this improvement, proof generation and verification require either two exponentiations per block (re-encrypting the ciphertext of the block's ``sum'' with claimed randomness) or three exponentiations (one for proof generation, two to verify the zero-knowledge proof). Therefore, to verify all the blocks of one mix-node would require either $2\frac{n}{\sqrt[m]{n}}$ exponentiations or $3\frac{n}{\sqrt[m]{n}}$ exponentiations for all blocks of a mix-node (where *m* is the total number of mix-nodes). Both improve upon the $6\frac{n}{\sqrt[m]{n}}$ exponentiations needed by Puiggalí et al. to generate the proofs (two exponentiations) and verify (four exponentiations) each of them for *n* ciphertexts and *m* mix-nodes.

Introducing parallelisation: During the mixing process, every mix-node of the mix-net re-encrypts and shuffles the input ciphertexts. The original idea of Puiggalí et al. was to process the encrypted votes by one mix-node after the other. It is possible to speed up this process by parallelizing in the following way: the set of input ciphertexts is divided into *m* subsets (where *m* is the number of mix-nodes). Then all mix-nodes start with one of the subsets and forward that to their neighbour after shuffling. This improvement[2] increases the efficiency by factor *m*. To ensure the privacy of the ciphertexts, even though they are grouped, the subsets should be selected for example by district or municipality.

Reducing trust assumptions: Optimal privacy in [AC10] is only ensured if all mix-nodes are honest. However, this is not the idea of a mix-net, where privacy should be ensured as long as one single mix-node is honest. Therefore, we propose building single mix-nodes similar to RPC where each mix-node shuffles twice.

Furthermore, correctness in [AC10] depends on the assumption that the verifier and the first mix-node do not maliciously collaborate. (Otherwise, the first mix knows what the block selection will be and therefore knows how to cheat undetectably). As such, it is essential for correctness that the challenge is unpredictable and generated after the mixing process. We sketch a method for ensuring this process.

[2] This improvement was implemented for the Norwegian voting trials.

Clarifying block sizes: The approach by Puiggalí et al. assumes that the total number of ciphertexts can be grouped in equally-sized blocks with block size $l = \sqrt[m]{n}$, for *m* mix-nodes and *n* votes. In general, there will be a remainder when computing *l*. We make this explicit[3] and incorporate its handling into our design.

4 Random Block Verification: Verifying Integrity of Random Blocks

In this section we describe *random block verification*, a mix-net with a detailed verification process, based on the proposal of Puiggalí et al., which includes all of the improvements proposed above.

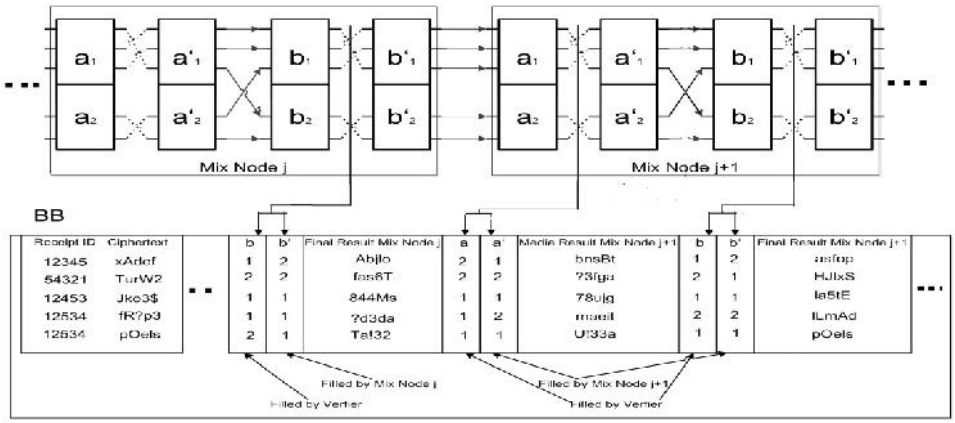


Fig. 2: Verification of one Mixnode for 5 ciphertexts, 2 blocks

Notation: In the remainder of this section, we consider *n* ciphertexts posted on the bulletin board and a mix-net consisting of *m* mix-nodes. We use the following notation: the set of input ciphertexts of mix-node *j* is C_j, the set of output ciphertexts after the first re-encryption/shuffling step is C'_j, and the set of ciphertexts after the second re-encryption/shuffling step is C''_j ,. During verification, C_j will be divided into *l* blocks a^j_1, $a^j_2, \ldots, a^j_l$. The corresponding output blocks (containing the same plaintexts) in C'_j are $a'^j_1, a'^j_2, \ldots, a'^j_l$. The input blocks for the second verification step are $b^j_1, b^j_2, \ldots, b^j_l$, and the corresponding output blocks in C''_j are $b'^j_1, b'^j_2, \ldots, b'^j_l$.

Mixing: For *m* mix-nodes the set of input ciphertexts is divided into *m* subsets. The j^{th} subset becomes the input of the j^{th} mix-node, which re-encrypts and shuffles the ciphertexts twice and publishes intermediate result C'_j and final result C''_j on the BB.

[3] The Norwegian implementation of [AC10] addresses this as well.

After mix-node *j-1* publishes its results, they become the input of mix-node *j* and the final result of the last mix-node *m* becomes the input of mix-node one. This is repeated until every subset has been mixed by all *m* mix-nodes.

Verification setup: The verification parameters are set as follows: the number of blocks *l* is determined by $l = \lfloor \sqrt{n} \rfloor$; there are $r = n - l^2$ blocks with *l +1* elements and *l-r* blocks with *l* elements. Verification begins by generating a random distribution of ciphertexts over verification blocks.

Distributing ciphertexts over blocks: Each mix-node is verified in an optimistic fashion: both input and output ciphertexts are grouped into blocks, and equivalence of the blocks is proven. As previously stated, if the assignment of ciphertexts to blocks is known to the mix-node prior to mixing, the mix knows how to cheat without being detected. Hence, this initial distribution must be generated randomly. Puiggalí et al. rely on an independent party to provide an initial random distribution. In contrast, we leverage the Fiat-Shamir technique [FS87] to group ciphertexts into blocks. Simply put, the first verifier computes the hash of its own output and uses that as the seed for a publicly-known random number generator. The resulting random stream is then used to assign ciphertexts randomly to blocks for the first mix (see Appendix A for details). As Fiat and Shamir point out [FS87], there is no way to tweak the input of the hash function to get a predictable output. Therefore, the resulting output is sufficiently unpredictable for the first mix and may be used as described. For all other mix-nodes *j*, the input blocks are determined by the output blocks of the previous mix-node *j-1*, meaning $a^j_1 = b'^{j-1}_1$, $a^j_2 = b'^{j-1}_2$, etc.

After dividing the input ciphertexts into blocks, the mix-node proves the correspondence between input block a^j_1 and output block a'^j_1, between input block a^j_2 and output block a'^j_2, etc. In the next step, the verifier distributes the ciphertexts of the output blocks $a'^j_1, a'^j_2, \ldots, a'^j_l$ over input blocks $b^j_1, b^j_2, \ldots, b^j_l$. As each block contains roughly as many ciphertexts as there are blocks, this is done to maximize privacy: the blocks of the input are chosen such that each input block b^j_y contains one ciphertext from every output block a'^j_x.
Of course, there are two block sizes: *l* and *l+1*. So (to be specific, the first *r* input blocks contain *l+1* ciphertexts) one ciphertext of every block and one additional ciphertext of block *r* (the first input block contains two votes of output block one, the second input block two contains two votes of output block two, etc.). All other *l-r* blocks contain *l* ciphertexts, one from each block. Then mix-node *j* proves the correspondence between output blocks $b^j_1, b^j_2, \ldots, b^j_l$ and input blocks $b^j_1, b^j_2, \ldots, b^j_l$.

Verifying blocks: To verify that a block of input ciphertexts was correctly processed by a mix-node, there are two options. Either the node reveals the sum of the used re-encryption random numbers (believed to be secure but not proven so), or the node uses the zero-knowledge proofs of [JJ99]. In either case, the node proves that the sum of the plaintexts of the block was not changed in the mixing step (Figure 2).

5 Analysis

In this section we analyse *random block verification* regarding fraud detection, privacy, and efficiency. In addition, the results are compared with those of *Randomized Partial Checking*, the *Proof of Subproduct* mix by Golle et al., and the "Norwegian mix" by Puiggalí et al.

5.1 Detecting malicious mixes

Optimistic verification is not a perfect approach – an error (e.g., changing a "1" to a "3") can be counterbalanced (e.g., 1 + 4 = 3 + 2) and pass undetected. To achieve undetected corruption of the mix result, a malicious mix has to change (drop, alter, insert) at least two ciphertexts in order to balance the introduced error. This will remain undetected *if and only if* the introduced errors are properly balanced within the same block. Since the division of ciphertexts into blocks is not known to the mix during mixing, the malicious mix cannot ensure this. Below, we investigate the probability of this happening by chance. As an aside, note that in any optimistic approach, a change must be counterbalanced. Therefore, to affect a change of *k* votes, at least one ciphertext extra has to be tweaked, leading to at least *k+1* changed ciphertexts. This is in contrast to RPC, where changes to ciphertexts cannot be balanced by other changes. That's why we compare the chance of changing *k* ciphertexts in RPC to *k+1* ciphertexts in optimistic approaches below.

Randomized Partial Checking: To cheat, a mix would have to drop/alter a ciphertext either in the first or in the second mixing stage. Since the mix has to reveal either the first or the second mixing stage, the chance of getting away with this is ½. Since this is independent, the chance of remaining undetected for *k* changes is

$$P_{rpc}(k \text{ undetected changes}) = 2^{-k}.$$

Proof of Subproduct: During the verification, α random blocks (for $\alpha \leq 5$) are generated with an average size of $\frac{n}{2}$ and compared with the corresponding output blocks. In case a malicious mix-node adapted *k* ciphertexts, the prover has to find another set of output ciphertexts that has the desired properties. The chance of doing this in polynomial time is at most $\left(\frac{5}{8}\right)^{\alpha}$ [BG02]. Thus a high number of used random blocks increases the probability that the modified ciphertext is checked. $\alpha = 5$ For instance, for $\alpha = 5$, the chance of getting away is $\left(\frac{5}{8}\right)^{5}$. The maximum probability of changing *k* ciphertexts without detection is reached at $\alpha = 1$ and is

$$P_{PoS}(k + 1 \text{ undetected changes}) = \frac{5}{8}.$$

Norwegian mix: Puiggalí et al. claim in [AC10] that the chance of not detecting that two ciphertexts have been altered by one mix is $(undetected) = \frac{l-1}{n-1}$, since the first ciphertext can be in any block, as long as the second is in the same. Using their proposal $l = \sqrt[m]{n}$ (with *m* being the number of mixes), gives the following chance of changing *k+1* ciphertexts without being detected:

$$P_{Norway}(k+1\ undetected\ changes) = \left(\frac{\sqrt[m]{n}-1}{n-1}\right)^k.$$

Random Block Verification: The chance of affecting a change of size *k* requires changing *k+1* ciphertexts. In the case of two changed ciphertexts, the RBV mix-net performs as good as Puiggalí et al. In case of more than two, the Norwegian mix-net performs slightly better, as their block size is inversely proportional to the number of mix-nodes, whereas ours is constant in this regard. Intuitively, our approach has $\sqrt{n}$ blocks of (almost) equal size, and therefore, the chance of a ciphertext occurring in one block is roughly $(\sqrt{n})^{-1}$. The chance of *k+1* ciphertexts occurring in the same block is therefore roughly $(\sqrt{n})^{-k}$. In reality, it is slightly better as some blocks are smaller than others. To be precise,

$$P_{rbv}(k+1\ undetected\ changes) = \left(\frac{\sqrt{n}-1}{n-1}\right)^k.$$

In RBV, the values for *m* and *l* are fixed at $m = l = \lfloor\sqrt{n}\rfloor$. As a result the correctness is independent of the number of mix-nodes *m*. In contrast the values for the approach proposed by Puiggalí et al. depend on the number of mix-nodes and are given by $l = \sqrt[m]{n}$ and $m = \frac{n}{l}$.

5.2 Privacy

In mix-nets, privacy is the question of how traceable a given ciphertext is through the mix-net. In general, there remains some imprecision: some output ciphertexts can be ruled out, but others may or may not be a re-encryption of the sought ciphertext. The size of the group that cannot be ruled out (which we will call "Anonymity group" or AG) provides a measure of how much privacy is achieved by the mix-net. In the following section we consider the case that only one mix-net is honest and keeps the input-output ciphertext relation secret.

Randomized Partial Checking: Depending on a coin flip, the verification procedure reveals either the link between an intermediate ciphertext and the input, or its link to an output ciphertext. In the worst case, the coin is completely fair meaning 50% of the links are linked with input ciphertexts and the other 50% with output ciphertexts.

Hence, $n/2$ output ciphertexts are not yet linked and must belong to the input ciphertexts whose link was revealed. Thus, for each ciphertext whose input link is revealed, the anonymity group size is $n/2$. A similar reasoning holds for ciphertexts whose output link is revealed. As such, the anonymity group of an RPC mix-net with one honest mix is

$$|AG_{rpc}| = \frac{n}{2}.$$

Proof of Subproduct: Using PoS, the ciphertexts are grouped in up to α random blocks (with α being the security parameter, $0 < \alpha \leq 5$). The authors show that the average anonymity group size is $\frac{n}{2^{\alpha}}$. Thus, increasing the security (i.e., the assuredness afforded by the verifiability) has an inverse effect on privacy: the larger α , the smaller the anonymity group. Consequently, PoS achieves the best privacy result for $\alpha = 1$, and the smallest amount of privacy is achieved for $\alpha = 5$ – in this case, $|AG_{PoS}| = \frac{n}{32}$. The most privacy PoS can grant in the case of only one honest mix is therefore

$$|AG_{PoS}| = \frac{n}{2^{\alpha}}.$$

Norwegian mix: The approach proposed by Puiggalí et al. reduces the block size dependent on the number of mix-nodes used. For *m* mix-nodes, a blocksize of $\sqrt[m]{n}$ is used. Thus, assuming that just one mix-node is honest the "anonymity group"' has a size of

$$|AG_{PoS}| = \frac{n}{\sqrt[m]{n}}.$$

Random Block Verification: In RBV, each mix-node is shuffled twice. For verification, the ciphertexts are grouped into blocks of size $\sqrt{n}$. So, after the first shuffle, the size of the anonymity group is $\sqrt{n}$. However, for the second process, the blocks for the second shuffle are chosen such that they include at least[4] one ciphertext of each of the output blocks of the first shuffle. Therefore, to trace the ciphertext through the second shuffle, *all* input blocks need to be considered, which means in turn that all output blocks need to be considered. Hence, for one mix,

$$|AG_{rpc}| = n.$$

[4] Since, in general, $\sqrt{n}$ is not a natural number, exactly one per block is not possible. However, our approach remains as close to that ideal as possible.

5.3 Efficiency

In determining efficiency, we only consider the number of needed exponentiations because these dominate the required computation time. The total number of needed exponentiations is determined by two components: proof generation by the mix-net and verification by the verifier. We compute the computational costs only for one mix-node. For re-encryption, our approach, like RPC, needs twice as many exponentiations per mix-node as the approach by Puiggalí et al. and PoS. That is because re-encryption and shuffling are performed twice, but the impact of this is reduced as the mix-nodes all process a subset of ciphertexts in parallel.

Randomized Partial Checking: During the verification of RPC two times the association between $n/2$ ciphertexts is shown. This can be done by revealing the random value , and it can be verified by recalculating the re-encryption. Therefore, two times $n/2$ exponentiations for the α -component of the ciphertext and two times $n/2$ for β -component of the ciphertext are needed. In total the computational costs per mix-node are

$$E_{rpc} = 2 \times 2 \times \frac{n}{2} = 2n.$$

Proof of Subproduct: The number of exponentiations during the PoS verification is $2\alpha(2m-1)$ [BG02] per mix-node (for a total number of *m* mix-nodes) and depends on the security parameter $\alpha \leq 5$. Therefore the maximum number of exponentiations per mix-node is $10(2m-1)$. Accordingly, the best efficiency is reached for α = 1 and is

$$E_{PoS} = 2(2m-1).$$

Norwegian mix: The verification process by Puiggalí et al. uses a zero-knowledge proof to show the correctness of every block. The computational cost to verify the plaintext equivalence depends on the number of blocks. For *n* ciphertexts, $\frac{n}{\sqrt[m]{n}}$ blocks are used. The calculation of the proof for each block requires two exponentiations and the verification of the correct mixing takes four. Therefore, the total number of exponentiations done by the mix-net and the verifier are

$$E_{Norway} = 6\frac{n}{\sqrt[m]{n}}.$$

Random Block Verification: The efficiency of our approach also depends on the number of blocks. For *n* ciphertexts, $m = \lfloor \sqrt{n} \rfloor$ blocks are used. During proof generation, it takes one exponentiation per block to calculate the witness.

It follows that for *m* blocks *2m* exponentiations are needed (*m* for each mixing step). Afterwards it takes the verifier two exponentiations per block to check the integrity of all blocks and thus *4m* exponentiations for both verification steps. This leads to a total number of

$$E_{Norway} = \mathbf{6}\frac{n}{\lfloor\sqrt{n}\rfloor}.$$

5.4 Conclusion

In Table 1, we summarise our findings. The ``Fraud'' row gives the chance of getting away with affecting the result with *k* votes (i.e., *k* changes for RPC, *k+1* changes for the others). Privacy is expressed in terms of the anonymity group of one mix, and efficiency is expressed in terms of the number of exponentiations. The bold numbers are the best scores in each row.

	RPC	*PoS*	*Puiggalí et al*	*RBV*
Fraud: P(undetected)	2^{-k}	$^{3}/_{8}$	$\left(\frac{\sqrt[m]{n}-1}{n-1}\right)^{k}$	$\left(\frac{\sqrt{n}-1}{n-1}\right)^{k}$
Privacy: |AG|	½ *n*	$^{n}/_{2}$	$\frac{n}{\sqrt[m]{n}}$	***n***
Efficiency: # exp.	*2n*	***2(2m – 1)***	$6\,\frac{n}{\sqrt[m]{n}}$	$6\,\frac{n}{\lfloor\sqrt{n}\rfloor}$

Table 1: Comparison (for *n* ciphertexts and *m* mix-nodes) of fraud detection (for one modified ciphertext), privacy and efficiency (for verification of one mix-node).

The table illustrates that RBV significantly improves privacy and efficiency over Puiggalí et al. at the cost of a slightly reduced ability to detect fraud. To get a feeling for how serious this reduction in fraud detection is, consider the following example. Consider 3 changed ciphertexts in a set of 1000 votes. The chance of not being detected is less than $\left(\sqrt{1000}\right)^{-2} \approx 0.1\%$.

6 Conclusions and future work

We discussed the mix-net verification scheme by Puiggalí et al., a mix of randomized partial checking (RPC) and optimistic mixing (OM). We highlighted several possibilities to improve efficiency, identified a privacy risk in case just one mix-net is honest (keeping the re-encryption and shuffling secret), and noted several ambiguities concerning verification block size and allocation of elements to verification blocks. We proposed an improved verification scheme, based on randomized partial checking of blocks, to address these issues. We provided a detailed analysis of the effectiveness (in terms of privacy, efficiency, and correctness) of our scheme and compared this with other schemes that enable a trade-off between privacy, correctness, and efficiency. We showed that the privacy and correctness of our scheme improve upon that offered by RPC and OM, as well as other approaches that offer a trade-off between efficiency, privacy, and correctness. In addition, our scheme is less computationally expensive than RPC. Specifically, our scheme provides a high probability of correctness for all elements at a low computational cost. This contrasts starkly with RPC, which validates some elements at an elevated computational cost.

There are several directions in which this work can be extended further. In this paper we did not address malicious inputs, e.g., in the case of a coerced voter. Finally, we're interested in applying this verification approach to improve the efficiency of an actual mix-net, such as Verificatum[5]. We also plan to discuss which probabilities satisfy legal requirements with legal scientists.

Acknowledgements: This paper has been developed within the project *VerKonWa* (Verfassungskonforme Umsetzung von elektronischen Wahlen) which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation) and conducted in cooperation with provet (Project Group Constitutionally Compatible Technology Design) at the University of Kassel and CASED (Center for Advanced Security Research Darmstadt).

Bibliography

[AC10] Puiggalí Allepuz, J., Guasch Castelló, S.: Universally verifiable efficient reencryption mixnet. In: Proc. EVOTE 2010. LNI, vol. P-167, pp. 241-254. GI (2010)

[BG02] Boneh, D., Golle, P.: Almost entirely correct mixing with applications to voting. In: Proc. CCS'02. pp. 68-77. ACM (2002)

[Cha81] Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2), 84-88 (1981)

[CP93] Chaum, D., Pedersen, T.: Wallet databases with observers. In: Brickell, E. (ed.) CRYPTO'92, LNCS, vol. 740, pp. 89-105. Springer (1993)

[DK00] Desmedt, Y., Kurosawa, K.: How to break a practical mix and design a new one. In: EUROCRYPT 2000. LNCS, vol. 1807, pp. 557-572. Springer (2000)

[5] http://www.verificatum.com/

[Elga85] Elgamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Proc. CRYPTO'84, pp. 10-18. Springer New York, Inc., New York, NY, USA (1985)

[FS87] Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Advances in Cryptology - CRYPTO'86. LNCS, vol. 263, pp. 186-194. Springer (1986)

[Gjo10] Gjøsteen, K.: Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380 (2010), http://eprint.iacr.org/

[GZB02] Golle, P., Zhong, S., Boneh, D., Jakobsson, M., Juels, A.: Optimistic mixing for exit-polls. In: Asiacrypt 2002, LNCS 2501. pp. 451-465. Springer-Verlag (2002)

[Gro10] Groth, J.: A verifiable secret shuffle of homomorphic encryptions. vol. 23, pp. 546-579 (2010)

[JJ99] Jakobsson, M., Juels, A.: Millimix: Mixing in small batches. Tech. rep., Center for Discrete Mathematics #38; Theoretical Computer Science (1999)

[JJR02] Jakobsson, M., Juels, A., Rivest, R.L.: Making mix-nets robust for electronic voting by randomized partial checking. In: Proc. USENIX'02 (2002)

[Neff01] Neff, C.A.: A verifiable secret shuffle and its application to e-voting. In: CCS'01. pp. 116-125. ACM, New York, NY, USA (2001)

[Sch91] Schnorr, C.p.: Efficient signature generation by smart cards. Journal of Cryptology 4, 161-174 (1991).

[SK95] Sako, K., Kilian, J.: Receipt-free mix-type voting scheme. In: Guillou, L.,Quisquater, J.J. (eds.) Proc. EUROCRYPT'95. LNCS, vol. 921, pp. 393-403. Springer (1995)

[TW10] Terelius, B., Wikström, D.: Proofs of restricted shuffles. In: AFRICACRYPT'10. LNCS, vol. 6055, pp. 100-113. Springer (2003)

[Wik03] Wikström, D.: Five practical attacks for "optimistic mixing for exit-polls". In: Selected Areas in Cryptography. pp. 160-175 (2003)

[Wik09] Wikström, D.: A commitment-consistent proof of a shuffle. In: Proc. 14th Australasian Conference on Information Security and Privacy, LNCS, vol.5594, pp. 407-421. Springer-Verlag, Berlin, Heidelberg (2009)

Appendix A

This section details how to arrive at a random distribution of ciphertexts over blocks.

Consider a setting with *m* mixes and *n* input ciphertexts, and thus with $l = \sqrt{n}$ blocks, identified as $i \in \{0, \ldots, l-1\}$. Of these, $r = n - l \times l$ are to have *l+1* elements, and the others are to end up with *l* elements. To ensure the initial assignment of ciphertexts to blocks is random, the first mix takes a hash of its input (by concatenating all ciphertexts), and uses the resulting number as seed of a random number generator. The stream of random bits from the generator is chopped into parts of size $s = \lceil \log_2 l \rceil$. Then, the first ciphertext is assigned to the block with the number given by the first part. Should this be a number greater than *l*, this part is dropped. The second ciphertext is assigned the block identified by the second part, and so on.

In case a part identifies a number for which there is no corresponding block, the part is dropped. When a block is full, its index number is dropped. Initially, blocks are considered full when they have *l+1* elements. As soon as *r* blocks have been filled, blocks are considered full (and their indexes dropped) when they have *l* elements. To speed up the assignment, the available blocks can be reindexed and *s* updated to limit the number of parts for which there is no corresponding block.

Session 3

Verification of E-voting

A Supervised Verifiable Voting Protocol for the Victorian Electoral Commission

Craig Burton[1], Chris Culnane[2], James Heather[2], Thea Peacock[3], Peter Y. A. Ryan[3], Steve Schneider[2], Sriramkrishnan Srinivasan[2], Vanessa Teague[4], Roland Wen[5], Zhe Xia[2]

[1]Victorian Electoral Commission,
Victoria, Australia
Craig.Burton@vec.vic.gov.au

[2]University of Surrey
Surrey, United Kingdom
{c.culnane, j.heather, s.schneider, s.srinivasan, zhe.xia}@surrey.ac.uk

[3]University of Luxembourg
Luxembourg
{thea.peacock, peter.ryan}@uni.lu

[4]The University of Melbourne
Melbourne, Australia
vjteague@unimelb.edu.au

[5]The University of New South Wales
Kensington, Australia
rolandw@cse.unsw.edu.au

Abstract: This paper describes the design of a supervised, verifiable voting protocol suitable for use for elections in the state of Victoria, Australia. We provide a brief overview of the style and nature of the elections held in Victoria and associated challenges. Our protocol, based on Prêt à Voter, presents a new ballot overprinting front-end design, which assists the voter in completing the potentially complex ballot. We also present and analyze a series of modifications to the back-end that will enable it to handle the large number of candidates, $35+$, with ranking single transferable vote (STV), which some Victorian elections require. We conclude with a threat analysis of the scheme and a discussion on the impact of the modifications on the integrity and privacy assumptions of Prêt à Voter.

1 Introduction

Australian elections have distinctive features that create unique challenges for automation. Almost all elections in Australia use preferential electoral systems. Both the alternative vote (AV) and the single transferable vote (STV) are common. Preferential voting offers voters a high degree of freedom to express their choices, but at the same time preferential voting can make it hard for voters to cast binding votes, and it is prone to voter error. Unintentional numbering errors are by far the largest category of errors contributing to informal[1] ballot papers—comprising 50% of the total informal votes in the 2010 Victorian state election.

To help simplify the voting, STV elections often provide voters with the option of selecting 'group tickets', which are predetermined preferences chosen by parties. This can result in large and complex ballot papers. For example in Victorian elections, the Legislative Council ballots have had up to 38 individual candidates and 11 group tickets.

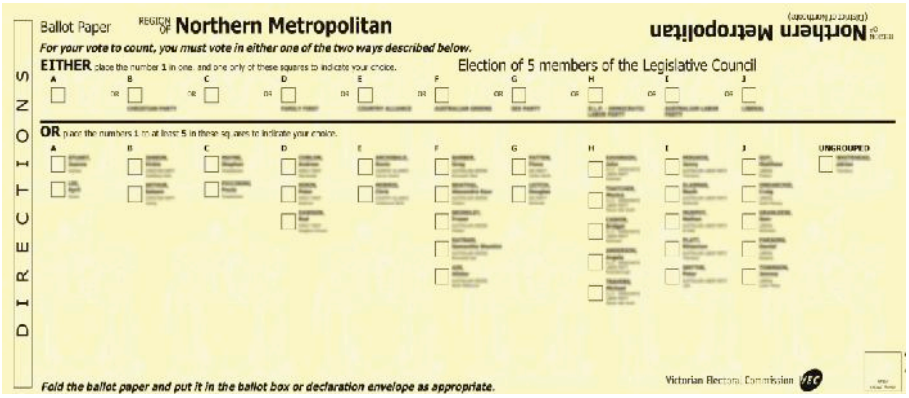


Fig. 1: Ballot paper for the Victorian Legislative Council

A sample ballot is shown in Figure 1. The ballot has a top section where voters can vote for a party or group (known as voting 'above-the-line'), and a bottom section where voters can mark their preferences for individual candidates (voting 'below-the-line').

There is a very tight turnaround for printing and delivering the ballots. Candidate nominations typically close on a Friday with Early Voting commencing at 4pm the same day. Ballots must be printed, checked, and delivered as soon as possible, but no later than the following Monday morning.

Another important characteristic of Australian elections is compulsory voting. This introduces numerous logistical challenges. For example, in state elections voters can cast their votes at any polling place in their state, which means that ballot papers for every

[1] by informal we mean any vote that is incorrectly filled and/or somehow ambiguous and non-binding

electorate must be delivered to each polling place before the voting commences, and then completed ballots must be returned to their correct electorates afterwards. Polling places are also set up overseas, usually at Australian embassies.

There is a strong onus on electoral commissions to provide a high level of accessibility for all voters. The complexity of preferential ballots causes difficulties for marginalized voters, in particular for voters with a print disability and voters from non-English speaking backgrounds. Many voters in these categories require human assistance to fill out their ballots, in which case there is no protection of vote secrecy. E-voting has the potential to help solve many of these problems. Although electoral commissions in Australia have generally been cautious about e-voting, there have been strong pushes toward adopting e-voting over the last five years.

The Victorian Electoral Commission (VEC) has been one of the early adopters of e-voting in Australia. In 2006, the VEC conducted a supervised e-voting system provided by a third-party vendor, and the system was rolled out on a larger scale in 2010. The e-voting system offered several benefits for both voters and the VEC. The voting machines alerted voters to numbering errors and could provide instructions in 12 different languages. All machines were equipped with audio facilities to provide guidance and feedback to vision impaired voters. The electronic nature of the ballots helped reduce the administrative overhead and physical security risks of returning the ballots through multiple third parties (couriers for instance); the ballots were submitted to centralized servers via a private network.

However, there were a number of concerns with this system. First and foremost, the system did not provide any meaningful verifiability of the votes. In addition, the proprietary nature of the system meant that none of the design and implementation details could be made public. The necessary, heavy customization of the vendor's core product (for instance to handle preferential ballots) created difficulties in tightly integrating the e-voting system with the VEC's existing election administration process (such as allowing general staff to run the entire system), and in deriving ongoing benefit from the supplier's core solution, which is on another development branch.
To address these shortcomings, the VEC decided to develop its own e-voting system in collaboration with the e-voting community. Academics from several universities are working with the VEC to design a suitable cryptographic e-voting protocol that provides both individual and universal verifiability. The design and the final system will be publicly available for peer review. The VEC's vision is for voters to cast their votes using the machines, which will provide (optional) take-home receipts for voters to verify their votes.

One of the main challenges is in finding the right balance between usability and security, in particular requiring voters to verify large amounts of information in preferential ballots and to perform cryptographic operations such as verifying digital signatures. Our main contribution is not in the proposal of the protocol, but more importantly in highlighting the difficulties and potential trade-offs in practice when applying cryptographic voting schemes to large-scale public elections that have specific requirements.

1.1 Related Works

The present work is based on the Prêt à Voter (PaV) electronic voting system [Rya04, CRS05]. The original PaV scheme has subsequently undergone various adaptations and enhancements, some of which are described elsewhere in this paper. The basic concept remains unchanged and is described as follows.
The voter receives a printed ballot as shown in Fig. 2 below. The order of the candidates is independently randomized for each ballot and the value "7*rJ*94*K*" represents an encryption of the order on the form.

Beta	
Gamma	
Alpha	
	7*rJ*94*K*

Fig. 2: A Prêt à Voter ballot form

At the polling station, the voter is given at random a ballot sealed in an envelope. She takes this to the booth, extracts the ballot form, marks the candidate of choice, separates the right-hand and left-hand sides (RHS, LHS) and destroys the LHS. She can now leave the privacy of the booth with the RHS of the ballot form. In the presence of officials and perhaps observers, the RHS is placed under an optical reader which records the information, that is, the value at the bottom of the strip and the position marked or the preferential rankings. The RHS, or a copy thereof, is retained as a receipt. Note that as the candidate order is randomized and has been destroyed, the receipt does not reveal her vote (except to someone possessing the decryption keys). The decryption keys are shared between a set of parties such that a certain threshold set of these parties is required to perform decryption. This ensures that no single party can decrypt all the ballots. Once all voting has ceased, the receipts are posted on a secure Web Bulletin Board (WBB). Voters can use this facility to confirm that their receipts appear correctly. A set of mix servers then perform a series of robust, anonymizing, re-encryption mixes (e.g. [Nef01, FS01, Wik10]) on the receipts so that the votes can be emitted and counted.

Although seemingly simple on the surface, the underlying protocol offers many of the properties desirable in voting systems such as ballot secrecy, individual and universal verifiability, and receipt-freeness. As PaV has a certain similarity to traditional pen-and-paper, booth-based voting, the user experience is familiar, making the scheme is readily adaptable to real-world situations.
The original scheme was designed for First-Past-The-Post (FPTP) voting as currently used in the UK, but it is clear that it adapts easily to ranked, AV, etc.: the voter simply adds further marks to the ballot. However, if done naively, this opens up possibilities of "Italian"-style attacks (see page 10). This has been addressed in [TRN08, XCH10], which introduce new mixing and tallying algorithms.
Certain fielded, verifiable voting systems, such as Scantegrity II [CCC08] and Civitas [CCM08], have the potential to accommodate ranked voting. However, it is unclear how they would perform with a large number of candidates. The checkerboard-style ballots in Scantegrity II would be impractical with $35+$ potential candidates. Encoding vote preferences in Civitas could incur a significant processing overhead when accounting for a sizeable candidate base. Furthermore, Civitas is a remote rather than supervised

scheme. Wombat (http://www.wombat-voting.com/) is currently implemented as an FPTP-supervised system, but again, it is unclear how it would handle a large number of ranked-vote choices. There could also be privacy issues connected to the plaintext audit trail provided by Wombat ballots.

With the PaV implementation for the VEC, we note that although workable solutions have been found for the moment, many research challenges remain. Whilst a formal security analysis has yet to be carried out, security of the scheme remains a primary concern throughout the development process and is being continuously monitored and discussed by all parties involved.

2 Front-End Design

We will now describe the proposed system.

2.1 Electronic Ballot Marking

In this section, we introduce the procedures of vote casting, in other words, how to record the voter's intent with an encrypted vote and how to verify that the encrypted vote has been correctly recorded by the election system.

Echo	θ_E
Bravo	θ_B
Alpha	θ_A
Delta	θ_D
Charlie	θ_C
$\{P\}$	

Table 1: Ballot form with voter's intent

An example ballot is shown in the above table. It contains a vertical perforation down the middle so that the two halves can be separated. The LHS lists the candidates in a random order. At the bottom of the LHS, is an unencrypted representation P of the candidate order, e.g., a computer-readable barcode. The RHS is left blank for the voter to mark her rankings. Moreover, on the RHS an encrypted value called an *onion* is associated with each candidate. If it is decrypted, its plaintext will represent the corresponding candidate in the LHS. The encoding of the onions is explained in section 3.

In contrast to the traditional PaV protocol, the voter does not mark her preferential rankings on the ballot directly. This is because the state of Victoria's upper house election contains around 36 candidates, and ranking so many candidates using a candidate list in the random order is obviously not user friendly. Instead, we will use a voting device called an *Electronic Ballot Marker* (EBM) to help the voter mark her rankings. The EBM is a standalone, isolated computer device with a barcode reader and touch screen. To cast a vote, the voter first inserts the ballot into the EBM, which will read the permutation information P in the bottom of the LHS. The EBM displays the ballot on its touch

screen interface such that the candidate list is in the official draw order. The user interacts with the touch screen to give her preferential rankings. Note that the EBM can also assist the voter by pointing out an invalid vote. Once the vote is confirmed, the EBM sorts the voter's rankings according to the permutation information *P* and prints the results on the RHS of the ballot.

The voter takes her completed ballot paper to a scanner. As with the conventional PaV, she separates the ballot along the perforation, destroys the LHS, and then feeds the RHS into the scanner. The scanner submits the voter's preferences and onions to the WBB, which will then generate a hash value of the received information and send the digital signature of the hash value back to the scanner. The scanner would then overprint the signed hash onto the RHS, which can then be taken away by the voter as her receipt.

The voter can choose to audit either the entire vote casting procedure or just a part. Here we explain how the complete auditing process should be carried out:

- *Audit the ballot:* This audit checks whether the ballot has been correctly generated. In other words, whether each onion on the RHS correctly encrypts the corresponding candidate on the LHS and whether the permutation information *P* contains the correct candidate order. A ballot either be audited or cast but not both. The auditing method is the same as the traditional PaV [CRS05].
- *Audit the EBM:* The EBM transfers the voter's rankings with respect to both the candidate list in the canonical order and to the candidate list printed on the ballot. This audit checks that the transformation is done properly. For example, the voter can randomly note down some or all of the candidate-preference pairs from the EBM's touch screen surface and then compare whether these pairs are consistent with those printed on the ballot.
- *Audit the vote recording:* This audit ensures that the encrypted vote has been correctly recorded by the WBB. To perform the audit, the voter calculates a hash value of the preferences and onions in her receipt and then checks whether the signed hash from the WBB is valid.

2.2 Digital Signature Issues

One of the fundamental principles of PaV is the issuing of a receipt that the voter can use to verify that their vote has been correctly recorded onto the WBB. It is this checking that assures the voter that their vote is being included in the count. If anything is amiss, the information on the receipt is incorrect or the information is missing from the WBB altogether, the voter can challenge the authorities. As such, the veracity of the receipt is vitally important.

A valid receipt provides protection for two parties: it provides the voter with evidence to launch an appeal while simultaneously protecting the system from false accusation. It is therefore essential that any issued receipt is verified by the voter when received. If it is invalid or false, the voter must appeal at that point in time. Once the voter has left the polling station, his or her right to appeal false receipts will have elapsed.
The difficulty is that it is easy to verify a digital signature on a computer but impossible for a human to perform such a calculation mentally. While at the polling station, the voter is virtually devoid of any trusted hardware and therefore does not have the ability to check the veracity of the digital signature in a way that is reassuring.

Alternative approaches have been suggested ([CBH11, Rya11]) that either augment or entirely do away with the digitally-signed receipt. Such schemes are based on verifying codes to ensure that the vote has been accurately recorded on the WBB. Such schemes have the desirable property that, upon leaving the polling station, voters will have already completed their verification step. However, such schemes do require a higher level of trust in the WBB, although there already has to be a certain degree of trust in the WBB due to the digital signatures. The bigger disadvantage is that the codes used to verify the recording of the vote must be distributed to the voter. The typical suggestion is to include them on the ballot form issued to the voter. However, this places a chain of custody requirement on those ballots, which, if breached, could potentially undermine the election's integrity. There may be situations where such a chain of custody already exists or where it is a preferred compromise to the digital signature approach.

The final and preferred option is to permit voters to use their mobile phones to verify the digital signature. Constructing a phone application to perform such a task is relatively easy: multiple organizations could work on providing such an application, allowing voters to use an app from an organization they trust or perhaps even build their own. Such an approach does require that the voter be in possession of a smartphone and that they sufficiently trust the device and the application to perform the operation. There is growing concern about malware on mobile devices, but currently the average user is likely to trust such a device. This approach also causes concerns about disenfranchising the poor or seniors, both groups that tend not to own smartphone devices. While this may be true, the validity of the system only requires a small number of people to check their receipt. Unless the machine/system can know in advance whether someone has a smartphone, it cannot risk cheating in case it gets caught. There may also be legislative problems with allowing phones and photographic devices to be used in a polling station; however, provided that the process is well-managed and audits be performed in a designated area, such concerns should be mitigated. It is worth noting that checking the signature can be performed at the polling station, in public, with assistance if necessary.

3 Back-End Design

In this section, we discuss how to tally the received encrypted votes into the election result.

We use the Exponential ElGamal cipher [ElG85] in our protocol. A plaintext message m will be encrypted as $E(m) = (g^m y^r, g^r)$. In the ballot form, there will be a ciphertext next to each candidate. Suppose there are k candidates in the election, the i -th candidate will be encoded as $E(M^{i-1})$, where M is a value larger than k (e.g. $M = k + 1$). A received vote will look similar to the following table (note that the columns might be in different orders, but the tally methods will not be affected):

Ciphertext	$E(M^0)$	$E(M^1)$	…	$E(M^{k-1})$
Ranking	R_1	R_2	…	R_k

Table 2: Received votes

3.1 Tally Method 1

We first sort the ciphertexts within the above table according to their rankings. The result will be a k -ciphertexts tuple $\{c_1, c_2, \ldots, c_k\}$ ranked in the canonical order. We then treat each of the ciphertext tuples as an input to the mix-nets (e.g. Verificatum [Wik10]). After the shuffle, all ciphertexts in the outputs are decrypted, and the election result will be calculated. However, the biggest drawback of this method is that the computational cost for the shuffle and decryption phase will be expensive if the number of candidates is large. Hence it is not ideal for elections with large numbers of candidates.

3.2 Tally Method 2

Alternatively, for a particular vote, we can use the homomorphic properties of the exponential ElGamal cipher to first absorb all the ciphertexts and their corresponding rankings into a single ciphertext as follows[2]:

$$E(m) = \prod_{i=1}^{k} E(M^{i-1})^{R_i} \quad \text{where} \quad m = \sum_{i=1}^{k} [\![R]\!]_i * M^{i-1}$$

[2] Note that in order to ensure the correctness of the election result, we need to ensure that m is always smaller than q which is the order of g . For 128-bit, 256-bit and 512-bit q , we can handle at maximum 27, 47 and 81 candidates respectively.

Then for each vote, we input the ciphertext $E(m)$ into the mix-nets. After the shuffle, all the ciphertexts will be decrypted. Hence, somewhere in the outputs, there will be a value g^m. In order to retrieve m from g^m, we can compile a look-up table for all ($m : g^m$) value pairs in advance (e.g. even before the tally phase starts). After the decryption, we search the table to retrieve the value m, and the ranking choice for this vote can be calculated using the value m.

This method is superior to *tally method 1* because the computational cost for the shuffle and decryption phase has been reduced to the minimum: for each vote, there is only one ciphertext to be shuffled and decrypted. However, the disadvantage is that we need to build a look-up table in order to retrieve the plaintext. For an election with k candidates, the look-up table will contain $k!$ different ($m : g^m$) values. So for elections with small numbers of candidates (e.g. Victoria's lower house election with around 7 candidates), to build such a look-up table is perfectly reasonable. But for elections with large numbers of candidates, it would be infeasible to build such a look-up table. For example, Victoria's upper house election will have $35+$ candidates, and the size of the look-up table for 36 candidates is $36! \approx 3.72 * 10^{41} \approx 2^{139}$.

3.3 Tally Method 3

The third tally method can be considered as a trade-off between the above two methods. It is specially designed for elections with a large number of candidates. We use Victoria's upper house election as an example to demonstrate the idea (we assume there are 36 candidates).
Similar to the *tally method 1*, for a received vote as shown in the table above, we first sort all its ciphertexts into a *k*-ciphertexts tuple $\{c_1, c_2, \ldots, c_k\}$, which is ranked in the canonical order. Now, starting with the first ciphertext in the tuple, we treat every t ciphertext as a group. Hence for the VEC election, if we set the size of the group $t = 6$, we can separate all 36 ciphertexts into $\frac{k}{t} = 6$ groups. As follows, we treat each group as t ciphertexts ranked from 1 to t.

The following processes will be similar to the *Tally Method 2*. For each of the t-size groups $\{c_{j*t+1}, c_{j*t+2}, \ldots, c_{j*t+t}\}$ where $j \in \left\{0, 1, \ldots \frac{k}{t} - 1\right\}$, we will absorb all the t ciphertexts into a single ciphertext using the homomorphic property as follows:

$$E(m_j) = \prod_{i=1}^{t} (c_{j*t+i})^i$$

Hence, we have packed a k -ciphertexts tuple into $\frac{k}{t}$ tuples of t -ciphertexts each as

$$\left\{E(m_0), E(m_1), \ldots, E\left(m_{\frac{k}{t}-1}\right)\right\}$$

Then, for each received vote, we input its $\frac{k}{t}$ and t -ciphertexts tuples into the mixnets. After the shuffle, all ciphertexts in the outputs are decrypted. Note that after the decryption, somewhere in the outputs, we only obtain $\left\{g^{m_0}, g^{m_1}, \ldots, g^{m_{\frac{k}{t}-1}}\right\}$, and we still need one look-up table to retrieve their plaintexts $\{m_0, m_1, \ldots, m_{\frac{k}{t}-1}\}$. This time, the size of the look-up table is $P_t^k = \frac{k!}{(k-t)!}$ which is much smaller than $k!$. In our case ($k = 36$ and $t = 6$), the size of the table is $P_6^{36} \approx 1.4 * 10^9 < 2^{31}$.

Above, we have shown a special case where $t|k$. In the case $s = k \pmod t$ where $s \neq 0$, the above method still works. Now, we can group the k ciphertexts into several t -sized groups and the remaining s ciphertexts are treated as a group. In such a case, we need to build two look-up tables, one with size $P_t^k = \frac{k!}{(k-t)!}$ to look up the t -sizes ciphertext groups, and the other with size $P_s^k = \frac{k!}{(k-s)!}$ to look up the s -sizes ciphertext group.

Therefore, thanks to this tally method, we are able to handle elections with a large number of candidates. We can carefully choose the value of t (how many ciphertexts should be absorbed into a single ciphertext) so that the size of the look-up table P_t^k is reasonable. Meanwhile, the shuffle and decryption phase is t -times faster than the *Tally Method 1*.

4 Discussion

In the previous sections, we tried to clarify the fundamental design ideas in a simple manner, leaving out some technical details and design decisions. In this section, we will discuss some of these issues.

- *Where are the onions stored? :* In section 2, we mention that on the RHS, an encrypted value, called an *onion,* is associated with each candidate. This implies that the onions are printed on the RHS. However, in order to achieve the proper security level, the size of each onion will be around 1KB. Obviously, it will be impractical to print 36KB data on the paper ballot. To solve this problem, we suggest that onions be recorded on the WBB and that they are linked to a particular ballot using a unique serial number.

- *Italian attack:* There are two kinds of an "Italian attack". The first type works for elections in which the voter can express her preference in a large number of ways. Coercers can force a voter to cast her vote in a unique way that no one else might use. Thus, if coercers find out that no one has cast a vote in this way, the voter will be caught. The second type works for elections in which the transfer history is revealed. Coercers can force a voter to rank an unpopular candidate before a popular candidate. Therefore, if the unpopular candidate is eliminated but there is no vote transfer to the popular candidate, the voter will be caught. The tally methods in this scheme are not able to prevent either kind of Italian attack, but this is a design decision; a tradeoff between security and efficiency. According to some recent works, several new schemes (e.g. [TRN08, BMN09, XCH10]) can prevent Italian attacks; however, their computational costs prevent them from being implemented in practice at the moment.
- *Ballot validity proof:* Generally speaking, in verifiable elections with homomorphic tallying, every ballot should contain some validity proof, which proves that each ciphertext encodes one of the pre-defined values. Otherwise, a faulty ballot could ruin the election result by introducing thousands of extra votes. In our design, although the homomorphic property has been used in the tally phase, it is only used to encode preferences within the ballot itself, not encode preferences across different ballots. Hence the ballot validity proof is not required. Any invalid ballot can only ruin itself: it could neither introduce extra votes nor ruin the other ballots.
- *Impact of the different tallying methods:* In section 3, although we have introduced three different tallying methods, the first two are just special cases of the last method. The major difference lies in how many ciphertexts can be absorbed into a single packing. Election authorities should choose this parameter based on different circumstances, and the selection will only affect the computational cost in the tallying phase rather than the security properties.
- *Vote packing using small primes:* There is an alternative method to pack the ranking information using small primes [PABL04]. For example, $p_1, p_2, \cdots, p_k$ are small primes representing each of the candidates, and $r_1, r_2, \cdots, r_k$ are their rankings respectively. Then the vote can be packed as $v = {p_1}^{r_1} * \cdots * {p_k}^{r_k}$. However, compared with the method we have introduced in the paper, this method has two drawbacks. First, when using small primes as counters, the aggregated value will grow very quickly as the number of candidates increase. If the said value is larger than p, it will be wrapped around by p, and we will still need a look-up table when retrieving the ranking choices. Moreover, this could also cause collision problems. Second, safe primes (primes of the form $p = 2q + 1$) need to be used so that small primes in G_q can be selected as the counters. However, this will result in a much larger q, making many calculations much slower. With our method, primes of the form $p = kq + 1$ where $k > 2$ can be used to speed up ballot generation and tallying without affecting security.

5 Security Properties

In this section we will briefly discuss how the modifications made to standard PaV impact the security properties normally associated with PaV. There are a number of security properties that are important to an electronic voting scheme. They are:

- Integrity
- Privacy
- Receipt-freeness
- Coercion Resistance
- Verifiability
- Usability

The integrity and receipt-freeness properties of the proposed system are identical to that of standard PaV. The manner in which the ballot form is filled out has changed, but not the underlying casting process or receipt construction. Likewise, the verifiability properties are transferable, provided that the voter performs the necessary checks, namely checking the overprinting and the digital signature. It could be argued that this is a more difficult task with the proposed system given the quantity of information that needs checking. However, the system does make it is easier to correctly complete the complex ballot form. The complexity of checking is a consequence of the complexity of the election, not the underlying system. While usability has improved in one sense, filling out the ballot, it may suffer in terms of how the overprinting approach will work. This requires further analysis and trials to determine how easy and reliable it is for the voter to perform.

The issue of robustness has been constantly considered and has influenced the design with aspects like the WBB peered among different parties. The robustness of the system is dependent on both the technology and the procedures surrounding it and is still being refined. The issue of requiring a network connection throughout the election in order to submit votes to the WBB and receive digital signatures back is a possible weakness. Various fallback options are being discussed and analyzed to determine the best compromise.

It is the privacy property that is most affected by the proposed changes. The system now utilizes an EBM that “learns” the vote. Strategies for mitigating this have been included, for example, enforcing that the EBM be offline and wiped clean at the end of the election. However, there is a new trust assumption here, that the EBM has been honestly setup and has not been compromised in any way to record and transmit the votes.

The issue of coercion resistance is impacted by the changes in privacy. Coercion resistance is far more complicated, since it also covers the perception of the voter. A weakening of privacy guarantees would likely reduce coercion resistance; such a discussion is beyond the scope of this paper.

6 Conclusion

In this paper we have presented an end-to-end verifiable voting scheme that would be suitable for use in a Victorian state election. We have detailed the modifications we would need to make to standard PaV in order to comply with the requirements of scale, usability, and legislation. In trying to move from theory to practice, modifications and compromises are a necessity. The challenge is choosing the right compromises and being able to adequately justify them. While some of these modifications are specific to the state of Victoria, for example above-the-line and below-the-line voting, the process we have undertaken is transferable to alternative scenarios.

Acknowledgements

This work has been partially funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under project 'TVS: Trustworthy Voting Systems' (EP/G025797/1) and the Luxembourg National Research Fund (FNR) under project SeRTVS-C09/IS/06.

Bibliography

[BMN09] Josh Benaloh, Tal Moran, Lee Naish, Kim Ramchen, and Vanessa Teague. Shuffle-Sum: coercion-resistant verifiable tallying for STV voting. IEEE Transactions on Information Forensics and Security, 4(4), 2009.

[CBH11] Chris Culnane, David Bismark, James Heather, Steve Schneider, and Sriramkrishnan Srinivasan. Authentication codes. Proceedings of the 6th USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'11), 2011. San Francisco, CA.

[CCC08] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. Proceedings of the 3rd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08), 2008. San Jose, CA.

[CCM08] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: toward a secure voting system. 2008 IEEE Symposium on Security and Privacy, 2008.

[CRS05] David Chaum, Peter Y. A. Ryan, and Steve A. Schneider. A practical voter-verifiable election scheme. Proceedings of the 10th European Symposium on Research in Computer Science (ESORICS'05), pages 118–139, 2005. LNCS 3679.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on IT, 31(4):467–472, 1985.

[FS01] Jun Furukawa and Kazue Sako. An efficient scheme for proving a shuffle. Advances in CRYPTO'01, pages 368–387, 2001. LNCS 2139.

[Nef01] C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. Proceedings of the 8th ACM Conference on Computer and Communications Security (CSS'01), pages 116–125, 2001.

[PABL04] Kun Peng, Riza Aditya, Colin Boyd, and Byoungcheon Lee. Multiplicative homomorphic e-voting. In Advances in Cryptology - Indocrypt 04, pages 61–72, 2004. LNCS 3348.

[Rya04] Peter Y. A. Ryan. A Variant of the Chaum voter-verifiable scheme. Technical Report of University of Newcastle, CS-TR:864, 2004.

[Rya11] Peter Y. A. Ryan. Prêt à Voter with confirmation codes. Proceedings of the 6th USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'11), 2011. San Francisco, CA.

[TRN08] Vanessa Teague, Kim Ramchen, and Lee Naish. Coercion-resistant tallying for STV voting. Proceedings of the 3rd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08), 2008. San Jose, CA.

[Wik10] Douglas Wikström. Verificatum, 2010. http://www.verificatum.org/verificatum/.

[XCH10] Zhe Xia, Chris Culnane, James Heather, Hugo Jonker, Peter Y. A. Ryan, Steve Schneider, and Sriramkrishnan Srinivasan. Versatile Prêt à Voter: Handling multiple election methods with a unified interface. In Indocrypt: 11th International Conference on Cryptology in India, 2010. LNCS.

Partial Verifiability in POLYAS for the GI Elections

M. Maina Olembo[1], Anna Kahlert[2], Stephan Neumann[1], and Melanie Volkamer[1]

[1]Center for Advanced Security Research Darmstadt
Technische Universität Darmstadt
Hochschulstraße 10
D-64289 Darmstadt
{firstname.lastname}@cased.de

[2]Universität Kassel
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Pfannkuchstraße 1
D-34121 Kassel
a.kahlert@uni-kassel.de

Abstract: We discuss the use of POLYAS, an Internet voting system, in GI (German Society for Computer Scientists (Gesellschaft für Informatik e.V.)) elections before 2010, in 2010 and 2011, as well as in the future. We briefly describe how the system was extended in 2010 to provide partial verifiability and how the integrity of the GI election result was verified in the 2010 and 2011 elections. Information necessary for partial verifiability has so far only been made available to a small group of researchers. In the future it would be ideal to make such information available to the general public, or to GI members, in order to increase the level of verifiability. We highlight legal considerations accompanying these possibilities, including publishing more details about the election results, the requirement for secret elections, avoiding vote buying, and how to handle complaints. Motivated by legal constraints, we propose further improvements to the POLYAS system. Finally, we generalize our findings for any partially-verifiable Internet voting system.

1 Introduction

Internet voting systems for legally binding elections have predominantly been black-box systems, e.g., Estonia's federal elections [MM06] and the elections for the Austrian Federation of Students [KET10]. One needs to trust that these systems work as they should, which is not ideal for elections. The GI – German Society for Computer Scientists (Gesellschaft für Informatik e.V.) - has also used such a black-box Internet voting system, POLYAS, to conduct its elections since 2004. In 2010, modifications were proposed to introduce partial verifiability in POLYAS [OSV11]. While partial verifiability may not be considered optimal, the assurance it offers to voters is likely to increase their trust in election results. However, only a small group of researchers has been able to verify the processes for the GI elections in 2010 and 2011. Obviously, there is a need to

make partial verifiability available to the general public or at least to GI members. However, public verifiability requires publishing information that was previously kept secret. We address this from a legal point of view and provide recommendations for future GI elections.

Furthermore, we identify a flaw in [OSV11] that allows an attacker to coerce voters as a result of publishing information needed to partially verify the election process. We propose a technical improvement that significantly mitigates the risk of the outlined attack. While the addressed issues with respect to partial verifiability can be overcome by technical means, the handling of complaints remains an open problem. We therefore recommend partially implementing the proposal of [OSV11] for future GI elections. Our findings regarding the handling of complaints are generalized for any partially verifiable voting system.

In section 2 of this paper, we provide background information on the POLYAS voting system and its use in the GI 2010 and 2011 elections. Section 3 looks at challenges arising from making partial verifiability publicly available by publishing details of the election results. In section 4, we discuss the risk of vote selling, which is likely to occur when the general public can verify the processes as researchers did for the 2010 and 2011 elections. Section 5 focuses on our proposal addressing the publishing of hash chain information for the purpose of integrity with respect to the risk of coercion. Section 6 analyzes complaint handling, and we conclude in section 7 with a statement on these challenges and present future work.

2 Background

First, we provide our definitions for verifiability and then review the POLYAS system, discussing how partial verifiability is provided, and finally look at the application of partial verifiability in the GI 2010 and 2011 elections.

2.1 Verifiability

Verifiability can be categorized as *universal verifiability* and *individual verifiability*. We use the definitions given by [OSV11]. Individual verifiability focuses on the voter and enables him to verify that his vote has been properly prepared and sent to the voting server (cast as intended) as well as stored, unaltered, in the ballot box (stored as cast). Universal verifiability enables any interested party to verify the proper tallying of all votes stored in the ballot box.

2.2 The POLYAS Voting System

The various components of POLYAS are discussed in this section. We look at the protocol that runs during the voting phase including one special mechanism, the hash chain mechanism, and the post-voting phase of the protocol.

Components: POLYAS is made up of the electoral registry server (*ERS*), the validation server (*VS*), and the ballot box server (*BBS*). An off-line tallying component (*TC*) is used to tally votes (loaded in an encrypted state from *BBS*). A discussion on how these components work is presented in [RJ07] and [MR10]. In a GI election set-up, the *ERS* is administered by the GI at a computing center, while all other components are located at Micromata.

Voting Phase: A voter authenticates him- or herself at the election website using a personal voter ID and voting TAN (received via postal mail). These credentials are verified by the *ERS,* which forwards the TAN to the *VS.* The *VS* checks its database for this particular TAN and generates a random voting token (VT) if the TAN is valid and no VT has previously been generated for this voter. The *VS* then sends the voting token to the *BBS* and *ERS*. The *ERS* forwards the token back to the voter. The voter receives a ballot from the *BBS* and proceeds to mark the ballot for the desired candidates. This selection, along with the token VT, is sent to the *BBS* and the selection is stored for the final tallying only once the voter confirms his or her vote. The *BBS* informs the *ERS* that the voter corresponding to a particular VT has cast a vote. Then, the *ERS* and *BBS* delete the copy of the VT in order to maintain voter secrecy, and the *ERS* invalidates the voter ID to prevent double voting. The voter then receives confirmation of a successfully cast vote.

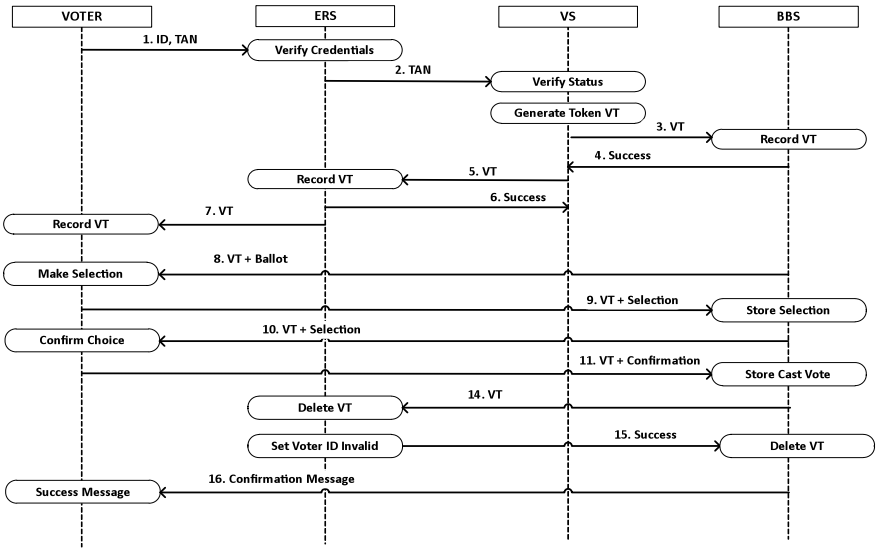


Fig. 1: A simplified view of the voting phase in POLYAS

Hash Chain: POLYAS uses a hash chain mechanism during the voting phase to enable integrity checks. Votes are encrypted once they are received, confirmed by the voter, and then stored in a randomized order in *BBS* in blocks of 30[1]. After receiving the first 30 votes, the *BBS* concatenates the encrypted votes, attaches an initial hash value in the first round, computes the hash using SHA-256, and signs the output using its private signature key. The output of the hash function and the signed version are sent to the *ERS* for storage. An acknowledgement message is sent back to the *BBS*. The next block of 30 votes is attached to this hashed output and SHA-256 is applied once again. This process is repeated for all available votes. If the last block of votes contains less than 30 votes, they are not included in the hash chain.

Post-voting Phase: At the end of the voting period, all encrypted votes are downloaded from the *BBS* and uploaded to the *TC*. The decryption key is input into the *TC* and all votes are decrypted and tallied.

This describes the original version of POLYAS, which does not provide any verifiability.

2.3 Partial Verifiability in POLYAS

A concept to enable partial verifiability in POLYAS was proposed in [OSV11]. A verifiability tool was developed and applied during the GI's 2010 elections and later extended to the GI's 2011 elections. The tool provides *universal verifiability* by taking the encrypted votes from the *BBS* and the decryption key as inputs, decrypting all the votes, and tallying them. The decryption key can be provided without violating secrecy of the vote, because there is no link between the encrypted vote and the corresponding voter. Assuming that the election results are published, the result obtained from the verifiability tool is compared to the result announced by the *TC*. This tool also facilitates partial *individual verifiability* through use of the hash chain. The encrypted votes and the initial hash value are required as inputs. The tool generates the hash chain information and compares the values obtained to those stored on the *ERS*. If there is any discrepancy, then manipulation can be detected. In this way, one can verify that after the hash value of a block is computed and sent to the *ERS*, votes in this corresponding block cannot be altered in the ballot box without detection, under the assumption that both the *ERS* and *BBS* do not collaborate. However, it must be noted that if a malicious *BBS* alters votes before they are stored in the ballot box and before the hash value is computed, then this would not be detected. Besides the verifiability tool, [OSV11] proposed that the *html* code be checked to verify that the vote has been cast as intended. Even with these extensions, POLYAS provides only partial verifiability as the process from receiving the vote and computing the corresponding hash value currently cannot be verified.

[1] The number of votes in a block is variable. The GI opted for 30 votes.

2.4 Application of the Verifiability Tool in the GI's 2010 and 2011 Elections

The GI holds elections once every year. In 2010, the election had a single race for the management board. There were nine eligible candidates and three positions to be filled. 3,193 voters participated via Internet voting and 51 voters by postal [2] voting. In 2011, the election had two races - for the presiding council and the management board. A voter could cast a "yes" or "no" vote for each candidate in the presiding council race and three votes in the management board race. In the 2011 election, 3,244 voters participated via Internet voting and 45 voters by postal voting.

The verifiability tool was used in the 2010 elections. After its extension to be used for two races, it was used for the 2011 elections. Both elections were successfully verified. For both of these elections, the GI opted not to make the information required to verify the election result publicly available. The interface specification which allowed implementation of the verifiability tool was only provided to researchers. Access to this information and the election data necessary to carry out verifiability required signing a non-disclosure agreement regarding the data provided and proprietary information on POLYAS.

In terms of verifiability, it would be ideal if this information was made available to all GI members or even to the general public. In addition, more information should be made available to further increase the level of verifiability. In the following sections, we discuss the legal and technical considerations for these extensions.

3 Publishing Complete Election Results

One consequence of enabling every GI member to verify his or her vote as described in section 2.4 is that voters could compute the number of selections per candidate, including the number of selections from Internet voters and those using the postal channel. This is possible because of the information available for verifiability and the published total result.

Until now, the GI only published the winning candidate's votes, preferring not to disclose the number of votes received by candidates who were not elected. Internet votes and postal votes are also not distinguished. In this section, we first consider legal requirements for publishing these details regarding the election results and discuss which body bears the responsibility of deciding whether to publish them or not.

[2] In this paper, postal voting also refers to voting by mail.

3.1 Is There a Legal Requirement to Publish Complete and Detailed Election Results?

In March 2009, the Federal Constitutional Court ruled that the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law - Grundgesetz - GG) requires that all essential steps in elections be subject to public examinability, unless other constitutional interests justify an exception [BVerG09]. Particular significance is attached here to the monitoring of the election act and to the ascertainment of the election result [BVerfG09].

However, private associations vested with legal capacity, like the GI, are allowed to regulate their elections and acclamations on their own [RGO09]. This is a result of the autonomy of association, a part of the constitutional principle of freedom of association (Article 9.1 GG) [El12]. As such, the association is free to regulate and formulate its affairs within the mandatory rules [Fl08]. This is regulated by law in § 25 of the Civil Code (Bürgerliches Gesetzbuch – BGB). § 40 BGB contains the right of the association to regulate their matters in articles of association according to their purposes [SSW10]. Therefore, the electoral principles (Article 38.1 in conjunction with Article 20.1 and 20.2 GG), which have to be observed at parliamentary elections, do not apply to associations' elections to the same degree, but the principles should fit with the autonomy of association [RGO09].

In matters associated with the proceedings of the GI elections, the autonomy of association of Article 9 GG is decisive. The legal arrangement of the electoral proceedings is delivered to the members of the association and can be specified by creating articles of association and subordinate electoral order in private autonomy [RGO09]. The GI availed itself of this opportunity by permitting electronic elections in § 3.5.4 of the articles of association and regulating particulars by implementing the Election Order (Ordnung der Wahlen und Abstimmungen - OWA) provision. Although § 3.5.4 of the OWA regulates the publication of the results, there are no rules about publishing the vote allocation, providing a listing of the results, and differentiating between postal votes and Internet votes.

Generally the elections of the management board and the presiding council are resolutions of the meeting of members according to § 32 BGB. However, the proclamation of a resolution of the meeting of members is not mandatory for the validity of a resolution [BGH75] [SSW10]. Even though it is stated in the articles of association that the organizer of the meeting of members, who is the returning officer, has to proclaim the resolutions of the meeting of members, this is generally considered just a regulatory action [SSW10].
As a result, an association, and in particular the GI, is neither compelled to publish detailed information about the election nor to distinguish between specific forms of elections when publishing the results; however, it is not forbidden. The remaining question therefore is to determine who can decide on publishing the election results. This is discussed in the following subsection.

3.2 Which GI Body is Allowed to Decide on Publishing Election Results?

The management board named in § 7.2 of the articles of association is the management board in terms of § 26 BGB and therefore the legal representative of the GI. This body is responsible for all of the GI's affairs that are not assigned to other bodies by the articles of association. The duties and authorities of the presiding council are mentioned in § 8.6 of the articles of association, including the decree about the implementing provisions like the OWA.

Since there is no regulation for publishing results, the GI could explain in the OWA to which extent election results are released to the public. The presiding council is responsible for modifying the OWA. Otherwise the management board is authorized to decide on the scale of the publication of electoral results because of the authority mentioned in § 7.2 of the articles of association. One could also decide to only provide access to GI members by publishing the results in the internal area of the GI web page.

4 Secret Elections and the Risk of Vote Selling

As it is generally possible to publish all relevant information for verifiability, in this section, we analyze whether the publication of the information required to verify future elections violates the secrecy of the vote.

4.1 Problem Description

In the GI elections, voters have multiple votes to cast and two races are held in parallel every second year. The risk of vote selling arises with such types of elections through the signature attack (also known as the "Italian attack"). In such an attack, a coercer [3] asks the voter to vote in an identifiable way for his preferred candidate. The voter would select the particular candidate and use the remaining votes to form a "signature" with his vote. Since the information to verify also enables a coercer to deduce all individual votes, he can confirm compliance with his instructions by searching through all the votes for the voter's "signature."

For the 2011 GI elections, given how POLYAS stores cast votes, there were 5,632 different possibilities to cast a vote.[4] This number of possibilities is obtained as follows: POLYAS stores the votes in the two ballots such that they can be linked to each other. The presiding council race had five candidates (a maximum of three could be selected), and another four candidates were available for the management board (for each candidate a "Yes" or "No" vote could be cast). An option for an invalid vote is provided on each ballot. POLYAS stores exactly what the voter selected, i.e., if in the first race the voter selected four candidates and the invalid option then this information was stored

[3] Coercer also refers to vote buyer.
[4] Note, only 3,244 votes were cast electronically.

exactly as selected. In the best case scenario, the coercer would ask a voter to vote for candidate *A* and create a signature along with this valid vote. The voter would then still have up to two selections to make out of four remaining candidates in the first race. In the second race, the voter votes either "Yes" or "No" for each option and whether or not to select the invalid option since the second vote can also be invalidated. This does not influence the first race and the vote for candidate *A*. The total number of possibilities for a unique signature is given by the equation below:

$$\#\,sig = \sum_{i=0}^{2}\binom{4}{i} \cdot \sum_{i=0}^{9}\binom{9}{i} = 5{,}632$$

In other words, 11 signatures from the first ballot times 512 signatures from the second ballot, with two being the maximum number of votes that remain in the first race for the voter to choose from, four is the total number of candidates the voter can now choose from in the first race, and nine is the number of vote options available in race two. Note, this attack was also possible with the postal voting approach used by the GI before Internet voting was introduced, when both votes were put in one envelope. GI members who were part of the tallying process and physically present at the GI headquarters in Bonn could search through all the votes to identify those which had the required signatures. As publishing the information to verify makes the data required for this attack more easily accessible, this attack would become much more attractive.

Similar to the discussion regarding publishing results, clarification is first needed on whether the GI's regulations require secret elections (this is not the case for all societies because members can also agree to non-secret elections).

4.2 Do GI Regulations Dictate Secret Elections?

Since associations are autonomous, they are allowed to form their own voting procedures as stated in Article 9.1 GG. The requirements for secret elections for associations differ from those for the elections of the Lower House of the German Federal Parliament (Bundestag) in virtue of Article 38.1 sentence 1 GG. If, however, an association opts for secret elections, the secrecy of individual voting decisions must be guaranteed [RGO09].

The GI Requirements for Internet-based Association Elections (*GI-Anforderungen an Internetbasierte Vereinswahlen*) [GI05], was adopted to the articles of association developed by a working committee of the GI's chairmanship. It declares that the secrecy of elections has to be ensured by mathematical methods and concepts of anonymity. This indicates that the principle of secrecy of elections is upheld by the GI and thus must be considered an election requirement.

According to the principle of the secrecy of elections under article 38.1, sentence 1, GG prescribes that the election procedure has to be carried out in such a way that the decision of the voter remains unknown [Sc09]. At the same time the secrecy of elections defends the freedom of election [Mo06]. The voter is protected from coercion and the candidate is safe from the postulations of 'his' voters.

Therefore, since the GI requires secret elections, the risk of vote selling based on the aforementioned signature attack is a problem for which a solution must be sought before making the verifiability information (as used in the elections in 2010 and 2011) publicly available.

4.3 Technical Solution Proposal

To mitigate the risk of the signature attack, we propose that the ballot be split into two ballots, one for each race, and stored in such a way that they can no longer be linked to each other. The number of possible signatures would be greatly reduced in the same scenario for the 2011 election in contrast to the scenario discussed above. There would only be 11 available signatures in the first race if the voter was coerced or sold his vote for candidate *A*. Note that in this approach, the second race cannot be used to create a signature as both votes will be stored independently and in such a way that they cannot be linked to each other. In the case where an adversary forces the voter to vote for candidate B in the second race, the coercer would only have twenty-seven possibilities to create signatures for valid votes:

$$\#\,sig = \sum_{i=0}^{3} \binom{3}{i} \cdot 2^{i} = 27$$

i.e., the voter can now choose up to three remaining candidates with a yes, no, or blank vote, thus there are three options. With this proposal, the adversary's number of possible signatures decreases significantly to 11 in the first race and 27 in the second race.

Another case, though not very attractive, is where the adversary forces the voter to cast an invalid vote (or buys an invalid vote). The number of possibilities to cast a vote for the second race [5] corresponds to 512, from which there are 431 invalid votes. To further improve the situation for this specific attack we propose that invalid votes are stored with no further information about the selected candidates, that is, there is no need to store further information from the ballot other than that the voter made an invalid vote selection. This proposal reduces the number of possibilities the adversary has available to demand invalid votes to one, thus the attack is no longer possible.

From a legal point of view, these technical solutions are an improvement as secret elections are further ensured. It remains to be seen if it is sufficient in the case of a judicial review.

[5] We focus on the second race as the problem is more obvious in this race.

5 Publishing Hash Chain Information

In the 2010 and 2011 elections, the hash chain information, which was stored on the *ERS,* was only provided at the end of the election. Thus, one needed to trust that the *ERS* and *BBS* did not collaborate to modify the ballot box (*BBS*) and the hash chain (*ERS*) accordingly. However, it would improve the level of verifiability if the hash chain information would be provided on a real-time basis on a public web page (*Bulletin Board - BB*), even if only accessible by GI members in the internal GI portal[6]. In this way, the members would be able to verify that no votes were modified after being included in the hash chain. As such, the assumption that the *ERS* and *BBS* do not collaborate would no longer hold because a modification of the database with the encrypted votes and the corresponding hash values would be detected as these values would not match with those on the BB. However, the idea of publishing this information immediately also has a drawback, which is discussed in the following subsection.

5.1 Problem Description

One drawback to providing the hash chain information on a real-time basis is the fact that a voter would know in which block his or her vote is stored as the voter could visit the BB before casting a vote, for example, for candidate *A*, and then observe that currently *x* hash values are published. He would then be able to tell a coercer that he voted for candidate *A* (as demanded by the coercer) and that his vote was stored in block *x+1*. The coercer would decrypt the votes at the end of the election and check on the votes in this specific block to verify the statement (again this is possible due to the verifiability discussed in sections 2.3 and 2.4).

In this scenario, a coercer only has to access the 30 votes in a given block while there would be 11 possibilities to cast a vote in the first race and 27 for the second race in total. Thus, the signature attack would again become more attractive if the hash chains are already being published during the election.

From a legal perspective, this is not acceptable in order to preserve secret elections. Therefore, we discuss possible improvements in the following subsection.

5.2 Technical Solution Proposals

To avoid disclosing this information, publishing the hash chain information could be delayed. A voter would then not know exactly which block contained his or her vote as several would be released simultaneously. However, this would decrease the level of verifiability because it provides a larger time frame within which votes could be manipulated without detection.

[6] This fact depends on the decision of section 3.2.

A second proposal is to split the ballot further, distributing the individual votes across the ballot box database and the hash chain. Rather than storing the votes from an individual voter together in the database and hash chain, these individual votes for specific candidates are randomly distributed and stored. Thus, individual ballots cannot be reconstructed from the database and the hash chain, however, it would still be possible to tally the votes per candidate and to verify, at the end of the election, that votes in the ballot box have not been changed after the hash chain was computed. A voter knowing which block his vote is stored in has nearly no knowledge that can be used by a coercer, and is thus prevented from selling his vote or being coerced.

Note, this also means that the honest voter who has not been coerced has less information. If he wants to verify whether his vote is in the corresponding block at the end of the election, he would not be able to reconstruct his vote. However, this is acceptable since the hash chain is used to detect manipulation in the database after the hash values are published, which was the main motivation for introducing hash chains. This possibility remains unaffected.

The measures of protection discussed in this section above are taken to avoid disclosing potentially sensitive information. As such, publishing hash chain information without delay but modifying how information is stored is acceptable from a legal point of view with respect to the secrecy of the election.

6 Complaints

Other than secrecy requirements for the election, there is a second challenge with respect to publishing hash chain information during the election, that is, how to handle complaints regarding the verifiable information.

6.1 Problem Description

A voter may check for the block number before casting his or her vote, and then complain that his or her vote was not included in that particular block, e.g., he selected candidate *A* while none of the votes in this block contains a vote for candidate *A*. Note, even though the voter does not know which is his vote, he can deduce that none of the votes contained the selection of candidate *A*. This situation is particularly difficult to handle as valid and invalid complaints cannot be distinguished. A dishonest voter may also attempt to make a falsified complaint, e.g., by selecting a block where no vote for candidate *A* is included and claiming that his vote is missing. Therefore, an approach is needed to handle complaints in order to allow immediate publication of the hash chain information. We first evaluate who has the burden of proof and then discuss what can be used as proof to file a complaint and how it would be handled in the judicial system.

6.2 Who Bears the Burden of Proof?

The judgment of the German Federal High Court of Justice states that every breach of mandatory law or articles of association causes the invalidity of adjudication. If the breach does not concern mandatory rules but procedural rules, which do not concern superordinate interests but rather the protection of individuals, the decision only becomes void if the voter protests against the decision [El12].

Relating to an action of an association against one of its members, the Federal Court of Justice has ruled that the association must prove the conformance of a decision with the articles of association, if the association wants to derive rights from an acclamation and if the member claims adverseness of the acclamation [BGH68]. Conversely, a member filing an action for a declaratory judgment and claiming the invalidity of an association election has to prove non-conformance with the articles of association. If someone claims the invalidity of a registered decision, the burden of proof generally rests on him [El12], [BGH68].

For the GI elections, this means that only breaches of mandatory rules of the articles of association or of the implementation rules cause invalidity of the election decision. It is up to the court of justice to determine this in particular cases. Every member of an association is allowed to file an action for a declaratory judgment in virtue of § 256 of the German Code of Civil Procedure (ZPO) against the association and thus assert the invalidity of an election. In this case, the member bears the burden of proof to show a defect. Therefore, members must have the possibility to control the election. Correspondingly, they are able to recognize election defects and submit these defects within the proper time period in order to push for legal action.

6.3 What Can Be Used and Accepted as Proof for Complaints?

The data that the POLYAS system itself currently provides for verifiability cannot be used as proof. However, voters could try to use technical aids to prove their claims, capturing voting actions using video or screenshots. If such a video would cover checking the block and then casting a vote, it can act as a proof, though it is not clear whether videos or screenshots have been manipulated. Voters may present witnesses to confirm their statement, but due to the possibility of manipulation, it can be assumed that the court is unlikely to admit this as proof.

Since a voter is not allowed to reveal his own voting decision in court as it violates the secrecy of elections [BVerwG76], it seems impossible that a court will admit the examination of a third person as a witness because this would mean further breach of secrecy. The voter could insist on appearing as a witness in person by arguing that there is no other chance to provide evidence that the system malfunctioned. It is not possible to judge on the voter's experiences and problem description as valid complaints can still not be distinguished from invalid ones, and the voter himself cannot prove his complaint. By refusing this evidence, the court would deprive the voter of his legal protection

[MüKo2012] [7], and by rejecting all complaints, as voters are not able to provide concrete evidence under the system, courts would not be able to further examine complaints that are indeed valid. To avoid the uncertain result of a legal proceeding, the association could establish an internal structure to scrutinize elections. However, for the moment, it cannot be recommended to publish the hash chain information during the election as no corresponding regulation for the GI exists.

7 Conclusion

In the recent past there has been an increase in the use of Internet voting systems. While ideally these systems would provide the user with the possibility to verify the election outcome, many of those used in practice are black-box systems. Voters therefore need to trust the systems. One example of a black-box Internet voting system is the POLYAS system, used in GI elections since 2004.

In 2011, the authors in [OSV11] proposed an improvement to POLYAS. Their suggestion was to publish the election results and the hash chain information to increase the level of verifiability, which is referred to as partial verifiability. In this paper we analysed the legal considerations for the GI elections using this version of POLYAS. This includes the need to publish election results for all candidates. We showed that this is not clearly regulated under the GI operating framework and that the presiding council is in charge of this. We then discussed whether publishing the information proposed in [OSV11] violates the secrecy of the vote. We showed that vote selling or coercion using the signature attack becomes more attractive. As this caused legal concerns, we proposed splitting the ballots in multiple race elections in order to maintain secret elections and enable partial verifiability for future GI elections.

Even though publishing election results is justifiable under the modifications made, publishing hash chain information during the election may still suffer from signature attacks. Therefore, we presented a randomization concept that allows one to bind the ballot box server to its content, ensuring integrity while at the same time significantly mitigating the risk of voter coercion.

However, as the handling of complaints turned out to be an open problem, we do not recommend publishing the hash chain information during the election. Therefore, it is recommended to clarify whether results per candidate can be published. If this is the case, then the improved extension for POLYAS should be applied for future GI elections without publishing the hash chain information during the election.

Recently, discussions with the POLYAS developers began regarding the corresponding problems and legal restrictions. For the future, we plan to closely collaborate to resolve these challenges. Future work will investigate how complaints can be handled and if such complaints are only a challenge to voting systems that provide partial verifiability

[7] Rejecting all complaints as voters are not able to prove their statement with this system would also mean that valid complaints will not be examined further. This needs to be discussed in future work.

or also to voting systems that provide end-to-end verifiability. A look at Civitas [CCM08] offers a potential solution. Since vote updating is enabled, a voter can update their vote, rather than raise a complaint, if they detect manipulation. Thereby, responsibility for the vote casting process rests with the voter.

Bibliography

[BGH68] Bundesgerichtshof. In: Neue Juristische Wochenschrift (NJW) 1968; pp. 543-545.

[BGH75] Bundesgerichtshof. In: Neue Juristische Wochenschrift (NJW) 1975; p. 2109.

[BVerfG09] Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 123; p. 39.(70) http://www.bundesverfassungsgericht.de/entscheidungen/rs20090303_2bvc000307en.html.

[BVerwG76] Bundesverwaltungsgericht. In: Neue Juristische Wochenschrift (NJW) 1976; pp. 259-260.

[CCM08] Clarkson, M.R.; Chong, S., Myers, A.C.: Civitas: Towards a Secure Voting System. In IEEE Symposium on Security and Privacy, 2008; pp. 354-368.

[CF85] Cohen, J.D.; Fischer, M.J.: A Robust and Verifiable Cryptographically Secure Election Scheme. In 26th Annual Symposium on Foundations of Computer Science, 1985; pp. 372-382.

[El12] Ellenberger, J. § 25. In: Palandt, O.: Bürgerliches Gesetzbuch – Kommentar, 71. Auflage, Verlag C.H. Beck, München 2012.

[Fl08] Fleck, W.: Die virtuelle Mitgliederversammlung im eingetragenen Verein. In: Deutsche Notar-Zeitschrift (DNotZ) 2008; pp. 245-258.

[GI05] Gesellschaft für Informatik: GI-Anforderungen an Internetbasierte Wahlen; 2005 http://www.gi.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf

[KET10] Krimmer, R.; Ehringfeld, A.; Traxl, M.: The Use of E-Voting in the Austrian Federation of Students Elections 2009. In (Krimmer, R., Grimm, R.): Electronic Voting 2010, Proceedings of the 4th Conference on Electronic Voting, LNI GI Series, Bonn, Germany, 2010; pp. 33 – 44.

[Ko12] Koch. § 18 Betriebsverfassungsgesetz; In: Erfurter Kommentar zum Arbeitsrecht, 12. Auflage, Verlag C.H. Beck, München, 2012.

[Mo06] Morlok, M., Art. 38. In: Dreier, H.: Grundgesetz – Kommentar, 2. Auflage, Mohr Siebeck Verlag, Tübingen, 2006.

[MM06] Madise, U.; Martens, T.: E-Voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In (Krimmer, R.): Electronic Voting 2006, Proceedings of the 2nd International Workshop, LNI GI Series, Bonn, Germany, 2006; pp. 15 – 26.

[MR10] Menke, M.; Reinhard, K.: Compliance of POLYAS with the Common Criteria Protection Profile – A 2010 Outlook on Certified Remote Electronic Voting. In (Krimmer, R., Grimm, R.): Electronic Voting 2010, Proceedings of the 4th Conference on Electronic Voting, LNI GI Series, Bonn, Germany, 2010; pp. 109 – 118.

[MüKo12] Müller, H., § 107c. In: Münchener Kommentar zum Strafgesetzbuch, 2. Auflage, Verlag C.H. Beck, München 2012.

[OLGMü08] Oberlandesgericht München. In: Neue Zeitschrift für Gesellschaftsrecht (NGZ) 2008; pp. 351-353.

[OSV11] Olembo, M. M.; Schmidt, P.; Volkamer, M.: Introducing Verifiability in the POLYAS Remote Electronic Voting System. In: Proc. of the Sixth International Conference on Availability, Reliability and Security (ARES2011), Vienna, Austria, 2011; pp. 127 – 134.

[RGO09] Roßnagel, A.; Gitter, R.; Opitz-Talidou, Z.: Telemedienwahlen in Vereinen. In: MultiMedia und Recht (MMR) 2009; pp. 383-387.

[RJ07] Reinhard, K.; Jung, W.: Compliance of POLYAS with the BSI protection profile – Basic requirements for remote electronic voting systems. In (Alkasser, A; Volkamer, M.) E-Voting and Identity, 1st International Conference, (VOTE-ID 2007), Bochum, Germany. Lecture Notes in Computer Science, 2007; pp. 62 – 67.

[Sc09] Schreiber, W. § 1.: Bundeswahlgesetz – Kommentar, 8. Auflage, Carl Heymanns Verlag, Köln 2009.

[SSW10] Sauter, E.; Schweyer, G.; Waldner, W.: Der eingetragene Verein, 19. Auflage, Verlag C.H. Beck, München, 2010; Rn. 39a ff.

Session 4

Coercion Resistant E-voting Systems

Achieving Meaningful Efficiency in Coercion-Resistant, Verifiable Internet Voting

Oliver Spycher[1], Reto Koenig[2], Rolf Haenni[2], Michael Schläpfer[3]

[1]University of Fribourg
1700 Fribourg, Switzerland
oliver.spycher@bfh.ch

[2]Bern University of Applied Sciences
2501 Biel, Switzerland
{reto.koenig | rolf.haenni}@bfh.ch

[3]ETH Zurich
8092 Zurich, Switzerland
michschl@inf.ethz.ch

Abstract: In traditional voting schemes with paper, pens, and ballot-boxes, appropriate procedures are put in place to reassure voters that the result of the tally is correct. Considering that in Internet voting errors or fraud will generally scale over a much greater fraction of votes, the demand to get strong reassurances as well, seems more than justified. With the ambition of offering a maximum degree of transparency, so-called *verifiable* schemes have been proposed. By publishing the relevant information, each voter may verify that her vote is included in the final tally and that accepted votes have been cast using proper voting material. Remarkably, this can be done while guaranteeing the secrecy of the ballot at the same time. On the negative side, high transparency will generally make it easier for voters to reveal how they voted, e.g., to a coercer. In this paper we propose an Internet voting protocol that is verifiable and simultateously makes it practically impossible for vote buyers or coercers to elicit the voters' behaviour. We compare its efficiency with existing work under equal degrees of coercion-resistance using an appropriate measure (δ). The contribution of our scheme lies in its efficiency during the most critical phases of the voting procedure, i.e., vote casting and tallying. Moreover, during these phases, efficiency is insensitive to the desired degree of coercion-resistance.

1 Introduction

The secrecy of the ballot serves as a means to protect citizens from external influence that pressures them into casting a vote that does not reflect their personal preference. The key to protecting the secrecy of the ballot lies in preventing citizens from revealing to others how they voted. In traditional, paper-based schemes, precautions may require voters to fill out their ballots on-site, often in an isolated booth. Thus voters get the privacy it takes to render any information they take out of the polling station meaningless. Particularly, they cannot provide a coercer with a *receipt*, i.e., the information it takes to reveal the ballot they cast. In Internet voting, the quest for receipt-free, voter-verifiable systems is still ongoing. In a first phase, some propositions have been made that rely on strong assumptions, such as the existence of untappable channels [HS00] prior to the voting event. (In practice voters would need to register in person each time they are asked to vote using the Internet.) In 2005, Juels et al. achieved a

breakthrough by proposing a receipt-free and yet verifiable protocol under strongly reduced trust assumptions [JCJ05] (henceforth referred to as *the* JCJ protocol). Remarkably their scheme is not only receipt-free but also highly resistant to coercers who want to push voters into handing out their credentials, voting at random, or abstaining from casting a ballot. Schemes that succeed at circumventing these coercion attacks are called coercion-resistant.[1] For putting these advances in security into practice, Juels et al. still need to make strong assumptions regarding the computational power of the tallying servers. Such assumptions make implementing JCJ infeasible for large-scale elections, as shown in [CCM08].

Since 2005 there have been a number of propositions that take the work of Juels et al. as a starting point and want to make coercion-resistant Internet voting practical while also preserving the security features of JCJ [Ar08, ABR10, CH11, SKH11, SHK11]. With one exception, the propositions are configured to achieve high degrees of coercion-resistance at the cost of efficiency.[2] The price is always paid by either the voter or the tallying servers, which still have to perform lots of computing. This paper also proposes a protocol that is parameterizable regarding coercion-resistance. However, the price for a high degree of coercion-resistance is only paid during the setup-phase, i.e. the phase which is the least time critical. Notably, the computations related to the set-up phase specific to a vote only (*post-registration*) needs to be completed only after the last vote has been cast. We may expect voting phases to be typically long enough for post-registration to be completed, thus allowing the first vote to be cast just after the last voter has registered. Casting votes is just as fast as in JCJ, and tallying becomes drastically faster. We hereby address the general notion that user-friendliness and the possibility to obtain the election results early are preconditions for the successful introduction of Internet voting.

In Section 2, we provide an explanation of how coercion-resistance can be measured and how the JCJ protocol is considered coercion-resistant. After presenting our protocol, in Section 3 we compare its efficiency with the known proposals from the literature in Section 4 . Finally we make concluding remarks in Section 5.

2 Quantifying Coercion-Resistance

There are a variety of definitions for coercion-resistance. [KTV10] gives a nice overview of the various approaches. In their 2005 protocol proposition, Juels et al. included their own particular notion. The paper proves the protocol to be coercion-resistant in terms of their definitions. Subsequent JCJ-related protocols that were introduced under a formal view on coercion-resistance, have essentially done so using this model or one with slight technical adaptations.

---

[1] As it is common in the technical literature, we do not distinguish between vote buyers (people who give) and coercers (people who take). As far as we are concerned, a coercer is an algorithm designed to obtain the information it takes to reveal whether a voter has adhered to some predefined instructions.

[2] The only exception is the protocol proposed in [ABRTY10]. However, the scheme does not provide the same degree of verifiability as JCJ. This special case will be revisited in the context of Section 3.4 and Section 4.

All proposed protocols foresee the same defense strategy for the voter subjected to coercion: She hands out a fake credential to the adversary and casts the ballot of her choice through the anonymous channel using her real credential. In short, according to JCJ a protocol is coercion-resistant if an active, non-adaptive adversary cannot distinguish between dealing with the defense strategy and obtaining the real credential with a non-negligible probability of success. In order to prove the coercion-resistance of the JCJ protocol, the authors need to assume that along with the published result, the difference Γ between the number of cast votes n and the number of the ones that are actually counted (due to using a valid voting credential) gives the adversary no advantage in succeeding with coercion (*adversarial uncertainty*). As we will argue, adversarial uncertainty will always be low enough to allow coercion, even without any quantitative prior knowledge regarding Γ.

In [KTV10], Küsters et al. introduce their notion of a measure for quantifying coercion-resistance. They define the degree of coercion-resistance δ as the probability that the (reasonable) adversary will accept a run given that the voter submits to coercion minus the probability that the adversary will accept a run given that the voter applies the defense strategy.[3] They point out that there are opportunities of coercion already on the base of the expected and the effective tally, i.e., attacks that apply even in an ideal system. In that sense, JCJ seems justified in assuming adversarial uncertainty with regard to the expected tally. However Γ is a value specific to coercion-resistant Internet voting schemes. On one hand, since these schemes are not yet in practice, adversarial uncertainty with regard to Γ is to be expected in real life. On the other hand, since voters are also uncertain about Γ, the coercer can still launch an attack based on a wild guess $\Gamma = c$: he can offer money in case $\Gamma \leq c$ or scratch the car if $\Gamma > c$. The reasonable voter will then submit to coercion if she believes that the vote cast with the fake credential would cause Γ to exceed c by 1. Since in a scheme that is meant to be coercion-resistant there is no reason to actually take advantage of using fake credentials, c might initially be chosen relatively small, thus yielding a correspondingly high δ.

Given the exclusion of Γ from adversarial uncertainty, some parameterizable, JCJ-related protocols can be configured to achieve a degree of coercion-resistance that depends solely on the estimated Γ. However, in this case, the parameters have to be chosen such that no meaningful gains in efficiency as compared with JCJ remain. In any case, it seems that accelerating JCJ through parameterization inherently comes along with some loss in coercion-resistance. Nevertheless, this needs to be considered legitimate, knowing that JCJ would not have been considered coercion-resistant if adversarial uncertainty regarding Γ hadn't been assumed. Finally, it cannot be estimated whether coercion based on Γ promises less success than coercion based on the loss of coercion-resistance inherent to accelerating JCJ.

[3] If a vote buyer offers a voter 100 dollars for a vote when using a system that doesn't allow a defense strategy, the voter may expect to get the full reward when submitting to coercion and nothing otherwise. Intuitively speaking, δ signifies the fraction of the 100 dollars voters may on average expect to additionally get from a vote buyer when submitting to coercion as opposed to applying a defense strategy in a δ-coercion resistant system. Obviously, small δ values are what we are looking for.

The protocol we are about to introduce is δ-coercion resistant in a parameter β. We will compare its performance with others under parameters β that yield equal degrees of coercion-resistance δ, where δ signifies the reduction of coercion-resistance compared with the JCJ-protocol. Remarkably, unlike Γ, we are able to quantify δ for each of the protocols.

3 Protocol

Due to space constraints, we are not able to introduce JCJ beforehand. Instead we will indicate relevant divergencies from JCJ within our exposition. Due to the strong relation between both protocols, we find this approach to be justified. After showing the basic idea behind our protocol in Section 3.1 and presenting the applied cryptographic primitives in Section 3.2 , in Section 3.3 we start off by introducing a basic version of our protocol. It already holds strong security features. In Section 3.4 we will propose some slight enhancements to improve verifiability. We chose this step-by-step approach for the sake of readability. We will informally justify the δ-coercion resistance within the exposition of our protocol, i.e., assuming the ideality of the applied cryptographic primitives. The formal security proof is left for future work.

3.1 The Idea

Our scheme foresees the same defense strategy for voters under coercion as JCJ and the other well-known, verifiable, coercion-resistant protocols from the literature: they hand out an invalid credential and cast a vote to the public bulletin board (PB) using their real credential. The protocol should not enable the coercer to decide whether an invalid or a real credential was obtained, despite verifiability. Evidently this requires that the voters' be able to cast votes to the PB an arbitrary number of times, regardless of whether using real or invalid credentials.[4] As a consequence, the PB may contain multiple votes cast using the same credential as well as votes cast with an invalid credential. Thus all coercion-resistant protocols need to include steps to *remove duplicates* and *authorize votes* prior to decryption.
As in JCJ, our protocol divides the authorities put in charge of the voting system among *registrars* and *talliers*. Regarding corruption by a coercive adversary, we advise the reader to assume all registrars and a majority of talliers are trustworthy. This could be weakened by requiring that all registrars be trustworthy only during the registration step and during the other phases by assuming that each voter knows a registrar who will not participate in a coercive attack against the voter. This weakening requires no change to the proposed protocol and the reasoning strictly follows [JCJ05]. Regarding *verifiability* (defined in [JCJ05] as *strong verifiability*) none of the authorites need to be trusted. The definition requires voters to be able to detect the exclusion of legitimate votes, changes to legitimate votes, and the inclusion of multiple votes cast with the same credential. In Section 3.4, we will change this definition as well as give more power to voters during verification under the notion of *improved verifiability* (the features of which are also mentioned in [JCJ05] though not formalized), e.g., voters can additionally verify that all credentials used to cast votes are assigned to eligible voters, whereas the basic protocol

[4] If the number of accepted votes were limited, the coercer could test the received credential for validity by counting the number of times he can use it to cast a vote.

would only allow voters to verify this given respective trustworthy majorities of registrars and talliers. In order to achieve *improved verifiability* in the full protocol, we will enhance the basic protocol in Section 3.4 accordingly. The conclusion will be that our scheme reaches δ-coercion resistance and a degree of verifiability equal to the JCJ scheme, notably under equal assumptions regarding the authorities and adversarial power. After showing the applied primitives, we are ready to introduce our protocol.

3.2 Cryptographic Primitives

The new scheme applies the following cryptographic primitives: the ones not employed by the JCJ protocol are identified accordingly. In justifying coercion-resistance and verifiability in the course of our exposition, we assume primitives to be ideal.

Multi-party ElGamal Cryptosystem with Threshold. We propose all ciphertexts to be ElGamal over a pre-established multiplicative cyclic group $(\mathcal{G}_q, \cdot, 1)$ of order q, for which the decisional Diffie-Hellman problem (DDHP) is considered to be hard.[5] Assuming no decryption, ElGamal ciphertexts are not meant to disclose any information in the encrypted plaintext, even in the event that the plaintext space is small and in the presence of other ciphertexts.

We also propose the application of a multi-party computation scheme derived from [Pe91, GJK99] to preserve the confidentiality of encrypted values throughout the protocol. Thus, malicious decryption is only possible in the event of a conspiring majority (the number depends on the chosen threshold) of group members, i.e., registrars or talliers.

Verifiable Mix-Nets. Trustworthy mix-nets take an ordered set of ciphertexts and output re-randomized encryptions in a random order such that the link is not able to be retrieved. They are implemented as a sequence of shuffles, each performed by a distinct mix-node. The link between elements from input and output is only retrieved in the event of all nodes conspiring. Correctness of execution is proven using NIZKP.

[5] We thus follow Civitas [5], which basically instantiates the JCJ protocol. However they do deviate in the choice of the underlying cryptosystem. The reason behind JCJ choosing a modified version of ElGamal (M-ElGamal) lies in the reasoning of their security proof. Although we could allow our protocol to adopt M-ElGamal as well, we adhere to ElGamal, thus making its performance more easily comparable to most of the other known proposals for coercion-resistant Internet voting. Furthermore, the question whether to choose ElGamal or M-ElGamal does not seem sensitive to the design of a particular verifiable voting protocol but rather to the desired security reassurances of the cryptosystem itself. Notably, ElGamal has recently been proven to have the beneficial IND-CCA1 property (resistance against non-adaptive chosen ciphertext attacks) just as much as M-ElGamal [Li11]. Underlying our informal security argumentation within the protocol description, we assume that the plaintexts of all ciphertexts are unconditionally hidden, even when the plaintext space is restricted, and given the ideality of the remaining primitives.

Plaintext Equality Test PET. Given two ElGamal encryptions E_1 and E_2, the algorithm returns $true$ if the plaintexts are equal and $false$ otherwise. This is done by checking whether the decryption of $(E_1/E_2)^z$ equals 1 for a random value $z \in \mathbb{Z}_q$. [JJ00] PET is verifiable and reveals no non-negligible information on the plaintexts.

Additional Primitive M-PET. Unlike JCJ, the new scheme relies on an additional method for efficiently testing the equality among the elements encrypted by a set of ciphertexts as described in [We08]. Clearly, applying PET pair-wise on all elements of the set would result in quadratic runtime. This is exactly the approach chosen in the JCJ protocol and the reason for its inefficiency during the tallying stage.

Given ciphertexts $X_1, \ldots X_n$, the modified PET (M-PET) raises all values to a random value $z \in \mathbb{Z}_q$, and decrypts them to obtain the blinded plaintexts $x_1^z = DEC(X_1^z), \ldots, x_n^z = DEC(X_n^z)$. The blinded plaintexts can be efficiently compared for equality, for instance, by sequentially saving them in a hash table. If a hit is made, the algorithm returns as $true$ and as $false$ otherwise. M-PET doesn't reveal any non-negligible information on the plaintexts, given that the discrete logarithm of any plaintext x_i is unknown in the base of any plaintext x_j, $1 \leq i < j \leq n$.

Communication Channels. There is a public board PB which is used as a *public broadcast channel*. Voters post their votes to PB and the authorities post all output of the tallying phase to PB. For the sake of simplicity we also assume that all public information, including public values from the employed PKI, is accessible on the PB. Further there is an *untappable, authenticated channel* from the registrars to the voters to hand the voters their credentials. Finally an anonymous channel is in place to allow one cast votes anonymously to the PB.

Non-Interactive, Zero-Knowledge Proofs NIZKP. To provide verifiability, many computations throughout the protocol need to be paired with with non-interactive zero-knowledge proofs. These proofs allow voters to prove knowledge of a plaintext by proving plaintext membership of a given sub-domain of $\mathcal{G}_q$, authorities can also prove the correct execution of PET, M-PET, correct mixing, encryption and decryption. We rely on the Fiat-Shamir heuristic for secure non-interactivity, i.e., negligible knowledge-errors and overwhelming witness-hiding.

3.3 Basic protocol

Pre-Registration. The talliers jointly establish a multi-party ElGamal threshold PKI, publish their public key ε on the PB, and keep their shares of the corresponding private key to themselves. The registrars jointly establish a number of $\beta \cdot N_+$ random credentials, where β denotes the security parameter underlying the degree of coercion-resistance δ, and N_+ denotes the maximum expected number of individual voters ever to participate at elections hosted by the voting system. The credentials are tuples of the form (σ, i), whereas we use the terms σ-credential and i-credential to refer to the respective components. Each component is random from $\mathcal{G}_q$ and only computable if the registrars maliciously co-operate. They jointly encrypt and post each of the two components $(\mathrm{E}_\varepsilon(\sigma, \alpha_\sigma), \mathrm{E}_\varepsilon(i, \alpha_i))$ on the PB and memorize their share of the randomnesses α_σ and α_i, both random from Z_q. We call the resulting list of encrypted

credential components the *credential pool*. Finally, they pass all $E_\varepsilon(i, \alpha_i)$ through a mix-net and the talliers decrypt the output to form the list $\mathcal{UNL} < i >$, i.e., the list of i-credentials, the elements of which are unlinkable to the *credential pool* by the coercer. The pre-registration step is needed only prior to the first election hosted by the voting system. Since valid i-credentials need to be made public later in the protocol, the list $\mathcal{UNL} < i >$ is meant to enable voters, as in JCJ, to lie about their credentials directly after registering. The *credential pool* however will be processed at a later stage to allow the exclusion of votes cast with an invalid credential.

Registration. The voter roll is initialized as an empty list on the PB. After successful authentication for registration, the registrars choose an unassigned ciphertext tuple from the *credential pool* and post it to the voter roll along with an identifier of the voter. They hand voters their credential (σ, i), along with a proof that the credential corresponds with the ciphertext tuple. As with all computations by registars and talliers, this procedure is conducted by the means of multi-party computation, such that only a malicious collusion can compute the secret, i.e., the plaintexts. The proof is implied by one proof from each registrar computed by the respective partial knowledge of the randomness of α_σ and α_i. Finally, the voter secretly chooses the random elements $\hat{\sigma} \in \mathcal{G}_q$ and $\hat{\imath} \in \mathcal{UNL} < i >$. Whenever the coercer asks the voter to hand out her credentials, she can lie and hand out $(\hat{\sigma}, \hat{\imath})$. In the basic version of the protocol, the *voter roll* only serves as a reference for locating the unassigned credentials from the *credential pool* and for identifying the credentials to be retained in case voters lose eligibility.

Post-Registration. The registrars pass all the ciphertext tuples $(\mathrm{E}_\varepsilon(\sigma, \alpha_\sigma), \mathrm{E}_\varepsilon(i, \alpha_i))$ of the *credential pool* to a mix-net. From the output, the talliers decrypt the second component, the ciphertexts containing i-credentials. We call the resulting list $\mathcal{UNL} < E_\varepsilon(\sigma), i >$, as the coercer cannot link its elements to the credential-pool or to the non-anonymous voter roll. The post-registration step needs to be completed only prior to tallying, i.e., the phase in which voters cast their votes can be used for this step. Thereby the negative impact of the time-consuming mix-nets is mitigated, or even fully compensated, given that the voting phase is sufficiently long.

Vote Casting. The voter selects the representation c of her prefered candidate(s) from a set $\mathcal{C} \subset \mathcal{G}_q$, which we assume to be available on the PB. To cast the vote, she uses the anonymous channel and posts the two ciphertexts $A = \mathrm{Enc}_\varepsilon(\sigma, \alpha_A)$ and $B = \mathrm{Enc}_\varepsilon(c, \alpha_B)$ to the voting board on the PB, along with her i-credential in plaintext. The voter aditionally needs to post one non-interactive, zero-knowledge proof (NIZKP) per ciphertext. The first one requires voters to prove their knowledge of σ. This is done indirectly by proving knowledge of α_A. We thereby exclude the attempt to cast an illegitimate vote by undetectably copying and re-randomizing σ-ciphertexts from the PB.[6] The other proof shows that $c \in \mathcal{C}$. Since each authorized vote on the voting board will be decrypted during the tallying phase, requiring the second proof prevents coercers from forcing voters to select $c \notin \mathcal{C}$ according to some prescribed pattern, thus obtaining a receipt (*Italian attack*) [Di07] or from using the talliers as a decryption oracle to obtain σ-credentials for subsequent votes.

[6] Due to this measure, votes cannot be cast by stealing the credentials of other voters, given a trustworthy majority of registrars (a majority could still compute σ and i) and talliers (a majority could compute the private decryption key and decrypt $sigma$-credentials from list $\mathcal{UNL} - (E_\varepsilon(\sigma), i)$

Apart from casting the i-credential, this step is exactly the same as in JCJ. Although the coercer has no means of deciding to whom, among the uncontrolled voters, the i-credentials refer to, he still gains a quantifiable advantage at coercion. Recall that the voter under coercion had to choose an arbitrary value $\tilde{\imath}$ from $\mathcal{UNL} < i >$ and pretend that this was his i-credential. The reasonable coercer will therefore observe the voting board to find out whether someone has cast a vote using $\tilde{\imath}$. If this is the case, the coercer could conclude that $\tilde{\imath}$ is in fact an i-credential that belongs to another voter and that the voter under coercion has revealed a false credential.[7] The probability that a voter is unfortunate enough to choose $\tilde{\imath}$ is less than $\frac{1}{\beta}$. The further exhibition of our protocol shows that the coercer doesn't gain any additional useful information for distinguishing the behaviour of the voter under coercion. This will lead to the conclusion that our scheme is indeed δ-coercion resistant, when $\delta = \frac{1}{\beta}$.[8]

Tallying. At the beginning of the tallying step, the voting board contains tuples of votes (A, B, i) that might have been cast with wrong proofs, that were cast with the same credential as other votes (we call these votes *duplicates*), or that hold A- or i-components that do not correspond with a valid credential (σ, i) from $\mathcal{UNL} < E_\varepsilon(\sigma), i >$. Prior to decryption and counting, these invalid votes need to be excluded.

First, votes with wrong proofs as well as votes with i-credentials that are not contained as the second component of an element enlisted by $\mathcal{UNL} < E_\varepsilon(\sigma), i >$ are marked and excluded from further processing. In order to efficiently remove duplicates, the talliers only consider votes not cast with a distinct i-credential and apply $\mathrm{M-PET}$ on the A-components of votes cast with the same i-component.[9] At this stage a last-vote-counts or a first-vote-counts policy is enforced. Note that the steps described so far could also be performed each time a vote is posted, i.e., prior to the tallying stage.

To authorize votes, the i-credentials are used to link the A- and B-components of the votes with the encrypted σ-credentials from $\mathcal{UNL} < E_\varepsilon(\sigma), i >$ to form tuples $(E_\varepsilon(\sigma), A, B)$. These tuples are passed to a mix-net. We call the output $\mathcal{UNL} < E_\varepsilon(\sigma), A, B >$, since its elements are unlinkable to both $\mathcal{UNL} < E_\varepsilon(\sigma), i >$ and the voter roll and the votes on the voting board. For each element, the talliers apply PET to the first two components. If the algorithm comes back as *true*, A is an encryption of a valid σ-credential. In that case, the corresponding ciphertext B is decrypted and counted in the tally, otherwise the vote is excluded from further processing. Note that since votes are being assessed for the validity of σ-credentials encrypted by the A-component, we should not apply $\mathrm{M-PET}$ at this stage as such an approach would allow the coercer to

---

[7] Note, that this conclusion can only be drawn in the strict model proposed by JCJ, where it is assumed that exactly one voter is under coercion and that invalid credentials are only used to the degree of achieving adversarial uncertainty regarding Γ. If we now allow the coercer to believe that the vote cast with $\tilde{\imath}$ as the i-credential is a fake vote (one with an invalid σ-credential), coercion will become even more difficult. However, we adhere to the strict model proposed in the JCJ paper.

[8] The precise value of δ is $\frac{N_\perp - 1}{\beta N_\perp - 1}$. Firstly, this is always smaller than $\frac{1}{\beta}$ and secondly, the difference is very small and irrelevant for a reasonable $N_\perp$. We thus justify the facilitation of saying $\delta = \frac{1}{\beta}$.

[9] We hereby adhere to the approach proposed by Smith and Weber. However unlike Smith / Weber, we apply $\mathrm{M-PET}$ only when removing duplicates, not when authorizing votes as proposed by them. Since we do not check the validity of the values encrypted by A at the current stage, and since the coercer does not know the discrete logarithm of any valid σ-credential in the base of any other, the coercer learns nothing useful for his attack.

check the validity of $\hat{\sigma}$ by the means of another vote cast by him with an A-component encrypting, e.g., $\hat{\sigma}^2$, or in other words, a value the logarithm of which is known in base $\hat{\sigma}$. The basic protocol is illustrated in figure 1.

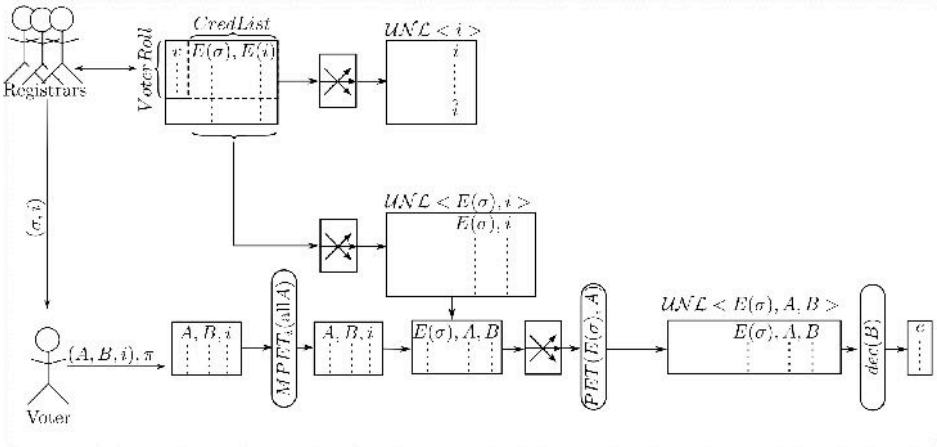


Fig. 1: Basic protocol

Credential Retention. As implied above, our scheme allows voters to re-use the same credential (σ, i) at numerous voting events. We therefore need to provide a mechanism that disallows voters to cast votes after losing eligibility, for instance when they leave the voting district. Removing their credential from the *credential pool* at post-registration is clearly not an option, since the coercer could verify the validity of the previously received i-credential by observing whether the value still appears on $\mathcal{UNL} < E_\varepsilon(\sigma), i >$ after the post-registration step of the following election. The protocol therefore defines credential retention by having the registrars compute a new σ-credential and replace $(\mathrm{E}_\varepsilon(\sigma, \alpha_\sigma))$ in the *credential pool* with an encryption of this new value. However, the encryption of the i-credential remains the same. Finally, the voter's ID on the *voter roll* is marked as non-eligible. The new credential in the *credential pool* is marked and may not be assigned to new voters, since the coercer would know the true value of the i-credential, in case it previously belonged to a voter controlled by him. Clearly, voters who have moved will not be able to use their retained credential for voting since such votes would be discarded upon *vote authorization*. Just as all unassigned credentials in the *credential pool*, the new credential can only be used for voting unnoticed in the event of colluding registrars or talliers (a case to be ruled out in the full protocol).

Now we observe whether credential retention gives the adversary an advantage at judging if the voter, who previously lost eligibility, lied to him. We consider two cases: 1) where the voter has submitted to coercion and 2) where the voter has applied the defense strategy. In the first case, the coercer would expect the distribution of Γ, i.e., votes not to be counted, to remain the same and the number of counted votes to decrease by one. In the second case, the coercer would also expect Γ to decrease by one. This is exactly the distinguishing factor we need to assume irrelevant by means of *adversarial uncertainty* when proving the coercion-resistance of the JCJ-protocol, i.e., independent of credential retention.

3.4 Full Protocol and Improved Verifiability

Evidently, the basic protocol complies with the definition of *verifiability* in the JCJ paper: it allows one to detect the exclusion of legitimate votes, changes to legitimate votes, and the inclusion of multiple votes cast with the same credential. Notably the definition already captures the commonly quoted requirement imposed on verifiable systems, i.e., that voters need to be able to verify that their vote has indeed been cast as intended, recorded as cast, and tallied as recorded. Regarding verifiability, our basic scheme is no less powerful than the well-known coercion-resistant scheme by Araújo et al. [ABR10, AFT07, Ar08]. However, the JCJ paper mentions that it may be desirable for any election observer to verify, that credentials have only been assigned to voters whose names are on a published roll. The JCJ-protocol does indeed provide this kind of verifiability. However our basic protocol only does so when assuming trustworthy majorities among registrars and talliers. In order to ensure that one can detect the event where registrars or talliers collude to cast votes with a credential enlisted by the *credential pool* but not by the *voter roll*, we propose an enhancement to the tallying step.

In the tallying step prior to decryption, the *voter roll* is passed to a mix-net which outputs the list $\mathcal{UNL} < E_\varepsilon(\sigma) >$. The coercer cannot link the entries of this list to the entries of the voter roll. After votes from $\mathcal{UNL} < E_\varepsilon(\sigma), A, B >$ with A-components that encrypt an invalid σ-credential have been excluded from further processing (at vote authorization as described above), the talliers apply $\mathrm{M-PET}$ on all A-components of $\mathcal{UNL} < E_\varepsilon(\sigma), A, B >$ and all entries in $\mathcal{UNL} < E_\varepsilon(\sigma) >$. If no collision is detected for any of the entries of the $\mathcal{UNL} < E_\varepsilon(\sigma) >$ for an A-component of $\mathcal{UNL} < E_\varepsilon(\sigma), A, B >$, the corresponding vote has obviously been cast with a credential that corresponds to an entry in the credential pool that has not been assigned to any voter. These votes are excluded from further processing, i.e., their B-components are not decrypted. The full protocol is illustrated in figure 2. Note, that since all input values to $M - PET$ are encryptions of valid σ-credentials, no discrete logarithm of any value in the base of any other is known. Therefore the coercer does not have any advantage, and it is justified to apply $M - PET$.

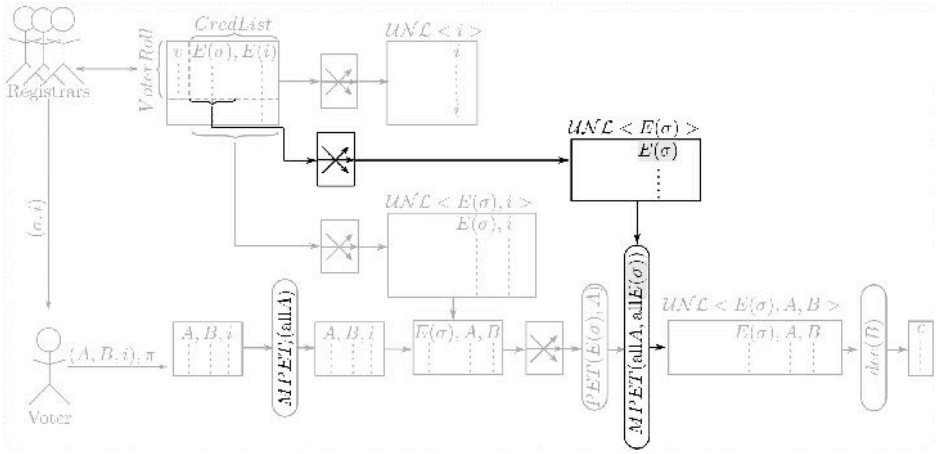


Fig. 2: Enhancement to the basic protocol to achieve full protocol

4 Efficiency

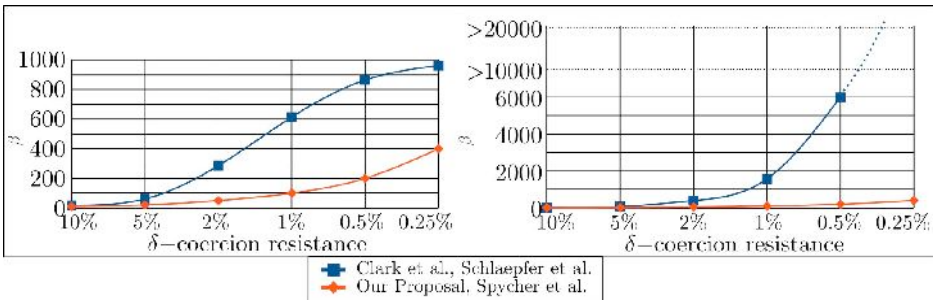


Fig. 3: The two drawings show the parameter β dependent on the degree of coercion-resistance δ. The diagram on the left shows the case for 1000 voters and 1000 votes on the voting board, the one on the right 100000 voters and 100000 votes on the voting board.

We now present the efficiency properties of our protocol through comparison with the schemes known from the literature. In the schemes by Clark et al. [CH11] and Schläpfer et al. [SHK11], voters associate their vote with non-anonymous information on the PB that refers to themselves. In order to mislead coercers, they randomly choose a set of other voters, who they can associate their vote with, thus forming an anonymity set of size β.[10] In the case of Clark et al., the *computation time on the voter's platform* scales in the parameter β. Particularly the number of modular exponentiations is $4 \cdot \beta + 10$, assuming a set $\mathcal{C}$ of two candidates to choose from. However, the tallying stage remains unaffected by the parameter and efficient, i.e., it is equally efficient as our basic protocol. The tallying time of our full protocol takes slightly longer, depending on the size of the mix-net but not more than twice as long. In Schläpfer et al. the *tallying time* scales in β, i.e., a mix-net during the tallying stage will need to perform $48 \cdot \beta \cdot N$ modular exponentiations, where N denotes the number of cast votes when assuming four mix-nodes.

The scheme by Spycher et al. [SKH11] does not rely on anonymity sets. Instead the registrar, who enjoys the voter's trust even after registration, assigns the voter an average number of β votes, under uniform distribution, cast with a false credential. Clearly this will also scale the time of tallying. $156 \cdot \beta \cdot n + 156 \cdot N$ is the number of modular exponentiation due to the most expensive steps, where n denotes the number of voters.

[10] In both cases coercion-resistance of degree $\delta = 0$ can be achieved by selecting $\beta = n$, where n is the number of voters. Moreover, it is sufficient for coerced voters to hide their votes in the anonymity set of size n, assuming adversarial uncertainty regarding the number of such votes. However this is a strong requirement, given large n.

Figure 3 shows the choice of β depending on the desired degree of coercion-resistance for the schemes with a corresponding parameter.[11] The scheme by Araújo et al. [ABR10] is by nature efficient at all stages and coercion-resistant with $\delta = 0$. However, as shown in Section 3.4 , it gives no means to verify whether authorities have created illegitimate credentials and cast extra votes.

We conclude that our protocol is efficient at both vote-casting and tallying. It does scale over β, but only during the non-critical pre-registration and post-registration steps. We therefore omit exact quantification. Furthermore, our protocol allows high levels of coercion-resistance, even under relatively small parameters. Since the pre-registration step may be conducted independent of the voting procedures, it will not have a negative impact on the elections. Also, the post-registration step can begin right after last voter has registered and only needs to end prior to tallying. The phase when citizens cast their votes should give enough time for completion.

5 Conclusion

It is true that the verifiable JCJ protocol offers coercion resistance but only under conditions that dot now allow such a protocol to be implemented for large-scale elections. Other proposed solutions either compromise verifiability or require a trade-off between coercion-resistance and efficiency during the critical phases of tallying vote-casting. Our proposal also requires more computation than conservative verifiable schemes; however, we have shown that when compared with other schemes, the factor that scales the computation time is small for relatively high degrees of coercion-resistance. Moreover, the expensive computations specific to coercion-resistance can be performed while the polls are open, i.e., while nobody is waiting.

Bibliography

[AFT07] R. Araújo and S. Foulle and J. Traoré. A Practical and Secure Coercion-Resistant Scheme for Remote Elections. In D. Chaum and M. Kutylowski and R. L. Rivest and P. Y. A. Ryan, editors, FEE'07, Frontiers of Electronic Voting, pages 330--342, Schloss Dagstuhl, Germany, 2007.

[ABR10] R. Araújo and N. Ben Rajeb, R. Robbana and J. Traoré and S. Youssfi. Towards Practical and Secure Coercion-Resistant Electronic Elections. In S. H. Heng and R. N. Wright and B. M. Goi, editors, CANS'10, 9th International Conference on Cryptology And Network Security in LNCS 6467, pages 278--297, Kuala Lumpur, Malaysia, 2010.

[11] In Section 3.3 we have shown that the coercion-resistance of our scheme follows $\delta = \frac{1}{\beta}$. It is easy to see that the same relation applies to the scheme by Spycher et al. as well. In the case of the protocols that rely on anonymity sets we have followed the definition from [KTV10]. To obtain δ, we need to compute $\sum_{r \in R} Prob(r|(\sigma,i)) - Prob(r|(\hat{\sigma},\hat{\imath}))$, where the condition in the first term signifies submission to coercion, the condition in the second one signifies applying the defense strategy. R denotes the set of results (i.e. the number of votes assigned to the voter under coercion) that the coercer would accept. Note, that inherent to assuming a reasonable coercer, the difference within the sum is inherently never negative. $\mathbf{Prob}(r|(\sigma,i))$ we compute as $F_1(r)$, where F_1 is the distribution function of a binomial distribution with N trials and a success probability of $\frac{\beta-1}{n-1}$, where N denotes the number of cast votes and n the number of voters. $\mathbf{Prob}(r|(\hat{\sigma},\hat{\imath}))$ we compute as $F_2(r-1)$, where F_2 again is the distribution function of a binomial distribution, this time with $N-1$ trials.

[Ar08] R. Araujo. On Remote and Voter-Verifiable Voting. PhD thesis, Department of Computer Science, Darmstadt University of Technology, Darmstadt, Germany, 2008.

[CH11] J. Clark and U. Hengartner. Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance. FC'11, 15th International Conference on Financial Cryptography, St. Lucia, 2011.

[CCM08] M. R. Clarkson and S. Chong and A. C. Myers. Civitas: Toward a Secure Voting System. SP'08, 29th IEEE Symposium on Security and Privacy, pages 354--368, Oakland, USA, 2008.

[Di07] R. Di Cosmo. On Privacy and Anonymity in Electronic and Non Electronic Voting: the Ballot-as-Signature Attack. Hyper Articles en Ligne, hal-00142440(2), 2007.

[GJK99] R. Gennaro and S. Jarecki and H. Krawczyk and T. Rabin. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. In J. Stern, editors, EUROCRYPT'99, International Conference on the Theory and Application of Cryptographic Techniques in LNCS 1592, pages 295--310, Prague, Czech Republic, 1999.

[HS00] M. Hirt and K. Sako. Efficient Receipt-Free Voting based on Homomorphic Encryption. In G. Goos and J. Hartmanis and J. van Leeuwen, editors, EUROCRYPT'00, International Conference on the Theory and Applications of Cryptographic Techniques in LNCS 1807, pages 539--556, Bruges, Belgium, 2000.

[JJ00] M. Jakobsson and A. Juels. Mix and Match: Secure Function Evaluation via Ciphertexts. In T. Okamoto, editors, ASIACRYPT'00, 6th International Conference on the Theory and Application of Cryptographic Techniques in LNCS 1976, pages 162--177, Kyoto, Japan, 2000.

[JCJ05] A. Juels and D. Catalano and M. Jakobsson. Coercion-Resistant Electronic Elections. In V. Atluri and S. De Capitani di Vimercati and R. Dingledine, editors, WPES'05, 4th ACM Workshop on Privacy in the Electronic Society, pages 61--70, Alexandria, USA, 2005.

[Li11] Lipmaa, Helger. On the CCA1-security of Elgamal and Damgard's Elgamal. Proceedings of the 6th international conference on Information security and cryptology in Inscrypt'10, pages 18--35, Berlin, Heidelberg, 2011. Springer-Verlag.

[Pe91] T. P. Pedersen. A Threshold Cryptosystem without a Trusted Party. In D. W. Davies, editors, EUROCRYPT'91, Workshop on the Theory and Application of Cryptographic Techniques in LNCS 547, pages 522--526, Brigthon, U.K., 1991.

[KTV10] R. Küsters and T. Truderung and A. Vogt. A Game-Based Definition of Coercion-Resistance and its Applications. Proceedings of the 23nd IEEE Computer Security Foundations Symposium (CSF 2010), pages 122-136, 2010. IEEE Computer Society.

[SHK11] Michael Schläpfer and Rolf Haenni and Reto Koenig and Oliver Spycher. Efficient Vote Authorization in Coercion-Resistant Internet Voting. 3rd International Conference on E-Voting and Identity (VoteID 2011), 2011. Springer-Verlag.

[SKH11] O. Spycher and R. Koenig and R. Haenni and M. Schläpfer. A New Approach Towards Coercion-Resistant Remote E-Voting in Linear Time. FC'11, 15th International Conference on Financial Cryptography, St. Lucia, 2011.

[We08] S. Weber. Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections. VDM Verlag, Saarbrücken, Germany, 2008.

Coercion-Freeness in E-voting via Multi-Party Designated Verifier Schemes

Jérôme Dossogne[1], Frédéric Lafitte[2], Olivier Markowitch[1]

[1]Computer Science Department, Université Libre de Bruxelles,
Bld. du Triomphe – CP 212, 1050 Brussels, Belgium
{jdossogn | Olivier.Markowitch@ulb.ac.be}

[2]Department of Mathematics, Royal Military Academy,
30 Renaissancelaan, 1000 Brussels, Belgium
Frederic.Lafitte@rma.ac.be,

Abstract: In this paper we present how multi-party designated verifier signatures can be used as generic solution to provide coercion-freeness in electronic voting schemes. We illustrate the concept of multi-party designated verifier signatures with an enhanced version of Ghodosi and Pieprzyk [GP06]'s threshold signature scheme. The proposed scheme is efficient, secure, allows distributed computations of the signature on the ballot receipt, and can be parameterized to set a threshold on the number of required signers. The security of the designated verifier property is evaluated using the simulation paradigm [Gol00] based on the security analysis of [GHKR08]. Unlike previously provable schemes, ours is ideal, i.e. the bit-length of each secret key share is bounded by the bit-length of the RSA modulus.

1 Introduction

Electronic voting is now a reality for national ballots (e.g. during the 2003-2004 referenda in Switzerland, some voters near Geneva were able to cast binding vote electronically [Sen04]; in Estonia, in 2009 more than 100 000 people voted through Internet for the local municipal elections; and the Estonian Parliament has recently opened the door for mobile phones to be used to authenticate voters in its 2011 election [Ric]), companies (e.g. it is common in shareholder elections in the United States to allow most voters to cast ballots via a web browser [Pro]), universities (e.g. to elect student representatives [Ass09]). Internet-based voting is a broadening trend [WV10]. The existing mechanisms of e-voting take different forms, from automated voting system to voting through networks. Recurring arguments are that electronic voting encourages a higher voter turnout and should make the counting of the ballots faster and more accurate. Whether using such technology in those contexts is a good choice or not is out of the scope of this paper. However, it is certain that electronic voting is a reality nowadays. Therefore, it is now mandatory to propose and to implement the technology to support essential e-voting systems requirements. For example, several properties are mandatory for a useful electronic voting system, such as ensuring the robustness of the system, the verifiability (i.e. ballots are published on a public bulletin board in a way that allow voters to verify the result of the election process), the anonymity of the voter, and

being coercion-free (e.g. Voteauction offered US citizens the chance to sell their presidential vote to the highest bidder during the Presidential Elections 2000, Al Gore vs. G.W. Bush [BKS+]). A number of contributions have described different ways to achieve robustness and verifiable electronic voting [DM10]. Problems arise when trying to combine voters' privacy with the ability for voters to check the correctness of their own votes by means of a receipt. Indeed, on the basis of such a receipt, a dishonest third-party could possibly force or encourage a voter to reveal his vote.

To avoid this weakness, some solutions [LK00] propose receipt-free voting protocols, but they are not problem-free. Some of these protocols can prevent the voters from being able to check whether their votes were counted, or they make it near impossible to report problems using evidence of the vote. Several schemes have been proposed to manage this problem, either by assuming that the voters must simply trust the polling office to behave honestly [LK00] or by paying more for data transmissions and computations overheads [HS00].

In a recent work, Juels et al. [JCJ05] and Backes [BHM08] present four different properties related to coercion resistance: receipt-freeness, immunity to simulation attacks, immunity to forced-abstention attacks, and immunity to randomization attacks. Essentially, coercion-freeness states that a coercer cannot force a voter to cast a certain vote or provide a receipt that would certify her vote. Intuitively, a protocol guarantees receipt-freeness if a voter does not gain any information that can be used to prove to a coercer that she voted in a certain way.

In this paper, while we intend to provide the voter with a receipt, we respect these four properties related to coercion resistance. However, our aim is to provide a receipt to the voter that he could use in court in case of conflict with the polling office. Nevertheless, we provide also the voter with the means to create his own receipts that are indistinguishable from a genuine receipt for an attacker but that cannot be used in a court since only the judge can distinguish between a valid receipt and one forged by the user.

The use of designated verifier signatures (DVS) by the polling office to sign the receipt, with the voter as designated verifier, is suitable to achieve such a feature [DM09a, DM09b, OMD04]. Jakobsson, Sako, Impagliazzo [JSI96] and Chaum [Cha96] introduced the notion of designated verifier signatures in order to strengthen the concept of undeniable signatures in Chaum and van Antwerpen [CV90]; their particular aim was to prevent blackmailing and mafia attacks [DGB87]. A valid designated verifier signature is such that it convinces only a specified recipient, while other entities would not be able to deduce anything about the validity of the presented signature. This can be achieved if the designated verifier of a signature s is able to produce a signature s′ intended for himself that is indistinguishable from s.

Furthermore, DVS can be generalized to allow multiple verifiers and are called Multi-DVS (MDVS) in such cases [SHCL08]. MDVS can be created based on ring signatures [LV04]; without encryption, based on [BGLS03]'s pairing-based ring signature [Lag07]; and on identity, based on [Cho08] a multi-signature extension of Hess's ID-based signature [Hes02] and Schnorr signature. MDVS suits e-voting very well since both the voter and a judge should be able to verify a signature created on a receipt at a polling office.
Multi-signer DVS (MSDVS) and their strong version MSSDVS [ZZZ08] are respectively a form of DVS where multiple signers are involved for a single designated verifier.

1.1 Our contribution

The aim of this paper is to introduce voting schemes in which each voter receives a receipt of his vote that cannot be used to reveal the vote to anyone except a judge. Therefore, such voting schemes, while they deter a coercer who might want to buy the votes, should allow the voters to verify his or her own vote but also to complain if necessary.

We propose a generic solution that relies on (w - 1,w)-threshold signature schemes and that allows coercion-freeness. Introduced in 1987 by Desmedt [Des88], a (t,w)-threshold signature scheme is a signature scheme where at least t participants out of w chosen entities have to cooperate using their own share of a common secret key in order to produce a valid signature. An attractive feature of most threshold schemes is that the shared key does not have to be known or reconstructed by the participants to produce the signature. Furthermore, there is no constraint on the number of participants that is needed in the verification process; therefore anyone should be able to verify the validity of the signature.

Based on a (w - 1,w)-threshold signature scheme, since any set of w - 1 out of the w participants can produce the signature, schemes can be created so that no one can deduce which one of the w - 1 participants participated in the signature generation. Hence all of the w participants can simultaneously deny their own implication in the signature generation. In such cases, everyone knows that only one of them would be honest when denying his or her implication; this provides us with the desired ambiguity.

Our objective, called source hiding and defined in [Lag07], is to transmit a receipt, r, for a ballot, b, from the polling office, P, to the voter, V, who cast b, that cannot be used by an attacker, A, to figure out the true content of b. We achieve this by creating a signature σ that can be produced either by P or by V, therefore, A can be sure that V did not create r to protect himself from A's coercion. At the same time, we want V to be able to ask a judge, J, to help him in case P did try to cheat him. This can only be achieved if r can serve as evidence for J, i.e. J can distinguish whether r was created by P or by V. In our construction, this is achieved by asking J to contribute to the signature creation, thus J would know whether the signature was created by V or by P.

MDVS is defined by [LSMP07] as a generic term for VS where "the signature is intended for n verifiers, n > 1". MSSDVS [ZZZ08], on the other hand, are DVS where multiple signers are involved. Since our construction's intent and purpose is to consider implicitly the signer J as verifier as well as V, and since both J and P are signers, it respects both properties based on those definitions1. [ZZZ08] illustrate the definition with a scheme based on bilinear pairing, whereas we will present a scheme based on RSA-PFDH [Cor02]. To avoid possible confusion with MDVS and MSDVS, we introduce the idea of multi-party designated verifier signatures (MPDVS).

Intuitively, we define tripartite multi-party designated verifier signatures in the following way: let P(A,B,C) be a protocol for Alice (A) to prove, with the help of Colin (C), the truth of the statement Ω to Bob (B). We say that Bob is a multi-party designated verifier if he can produce, with the help of Colin, identically distributed transcripts that are indistinguishable from those of P(A,B,C). This definition can be generalised to the multi-party case if we consider Colin as a set of co-signers called witnesses.

Multi-party designated verifier signatures are well suited for electronic voting schemes since those schemes can require an adjudicator to solve conflicts between the voter and the polling office and, as such, are tripartite by nature. If a voter systematically produces the indistinguishable transcripts every time he votes, an attacker who intercepts him after the voting procedure would not be able to know which of the receipts is the one corresponding to the real vote.

We illustrate our solution with an efficient, flexible multi-party designated verifier signature that is based on the threshold signature scheme of Ghodosi and Pieprzyk [GP06] and chosen for its simplicity and efficiency. We enhanced the scheme to make its security provable in the standard model while remaining ideal, i.e., the shared signing key's size is bounded by the size of an RSA modulus. At the same time, the proposed design facilitates distributed implementations of the computations and sets a threshold on the number of required signers.

The paper is organised as follows: In section 2 we present the notations, the adversarial model, and the security requirement for MPDVS schemes. In section 3 we describe an ideal and secure threshold RSA-PFDH signature scheme and use it to create a MPDVS scheme suitable for e-voting. In section 4 we analyse the security of that MPDVS and of the underlying threshold signature scheme. We conclude in section 5.

[1] The way Multi-DVS are defined and formalised imposes that "the participants …have to generate a shared RSA key"[LV04], "in identity-based cryptosystem, it also produces a master secret key (MSK), kept in secret by PKG (private key generator)"[Cho08]. This is not required in our primitive.

2 Model

2.1 Notation

The set of *w* participants (users) is denoted by U = {u1,…,uw}, where

u_1 is the polling office
u_2 is the voter
$u_3, \ldots, u_w$ are the witnesses

We also consider a trusted key generation server, denoted KGS. $A_u(x) = y$ means that the randomized algorithm *A* is run by user $u \in U \cup \{KGS\}$ and produces the output $y \in \{0,1\}^*$ on input $x \in \{0,1\}^*$.

S ⊂ U is the set of signers. We define $S_i \stackrel{def}{=} U \setminus \{u_i\}$ as the set of users that signs a message for the designated verifier u_i. In particular, we use the sets S_1 and S_2.

We write "$u_i \rightarrow u_j : m$" to denote that message *m* is sent from u_i to u_j via an authentic channel (tamper-resistant and authenticated).

$\sigma_{m,i}$ denotes the (partial) signature of user *i* on message *m*, $m_1|m_2$ is the concatenation of m_1 and m_2, $|m|$ is the bit-length of *m* and $m_1 \oplus m_2$ is the result of a bitwise XOR (exclusive disjunction) between m_1 and m_2.

Finally, since in our case $\sigma_{m,S1} = \sigma_{m,S2}$, indicating which *S* did sign is irrelevant, therefore we use σ_m to denote the usual RSA signature on message *m*. That is, $\sigma_m = m^d \bmod n$ where $ed = 1 \bmod \varphi(n)$ and $n = pq$. The prime numbers *p*,*q* are such that both their bit-lengths are approximately equal to the security parameter η.

2.2 Generic Description of MPDVS Schemes

A DVS scheme in which u_1 issues a signature for the designated verifier u_2 with help from witnesses $W = \{u_3,\ldots,u_w\}$ is defined as a set of five probabilistic polynomial time algorithms:
Setup $_{KGS}(\eta)$: Inputting security parameter η generates a master public key (MPK) and a master secret key (MSK). The MPK is transmitted to each user $u_i \in U$.

KeyGen $_{KGS}$(MPK,MSK): Using the master parameters, this algorithm generates the pair (vk_i,sk_i) for each participant $u_i \in U$ with vk_i as the public verification key and sk_i as the secret signing key.

$Sign_{u1,W}(m,sk_1,sk_3,\ldots,sk_w)$: This is a distributed process where u_1 and $W = \{u_3 \ldots u_w\}$ collaborate in order to sign message *m* for the designated verifier u_2.

$Sim_{u2,W}(m,sk_2,sk_3,\ldots,sk_w)$: This is a distributed process where u_2 and $W = \{u_3 \ldots u_w\}$ collaborate in order to sign message m for the designated verifier u_1. This algorithm generates a dummy signature that is indistinguishable from the signature returned by algorithm *Sign*.

$Vrfy(\sigma_m,m,MPK)$: Anyone can use this algorithm to check whether σ_m is a valid signature on m.

2.3 Security Requirements

The polling office u_1 signs the ballot sent by the voter u_2 with witnesses $u_3 \ldots, u_w$. This signature is like a receipt that all users can verify but that is only convincing to the voter (designated verifier): his ability to produce the same receipt makes it unconvincing for users that did not participate in the protocol.

Let's consider an active adversary who, before the execution of the protocol, is able to corrupt a fixed subset of at most $k < t$ users. By corrupting user u_i, the adversary learns the secret key sk_i.

The security definitions we use are taken from [LWB05] and adapted to our multi-party setting. DVS schemes are required to satisfy unforgeability and non-transferability as defined below:

- **Unforgeability:** If a signature is valid, then either u_1 or u_2 participated in its computation. This means that the threshold t must higher than the number of witnesses, otherwise the witnesses alone would be able to forge a signature.

- **Non-transferability:** When given a valid signature σ_m, it is infeasible to tell which users participated in its computation. In particular, it is infeasible to tell whether u_1 or u_2 participated.

In addition to these two properties, [LWB05] observes that some DVS schemes have the property of delegatability, which can lead to undesired situations for some applications. According to [LWB05], a DVS scheme is delegatable if the signer is able to reveal information other than her secret key (a function of that secret $y = f_i(sk_i) \neq sk_i$) that allows the attacker to produce a valid signature with regard to a single designated verifier. According to this definition, our scheme is non-delegatable. Indeed, the only information that the signer u_i could reveal, and that would allow the attacker to create such a signature, is her secret key sk_i. In this case, and contrary to [LWB05], non-delegatability follows from unforgeability.

3 Multi-party Designated Verifier Signature Scheme

3.1 The Ideal and Secure (t,w)-threshold RSA-PFDH Scheme

Our designated verifier scheme is based on Ghodosi and Pieprzyk's threshold signature scheme [GP06], which itself relies on Shamir's threshold cryptosystem [Sha79]. We adapted the scheme in order to provide a security analysis as strong as [Sho00, GHKR08], which is stronger than [GP06]. However, we maintain the same performance. Essentially, when creating shares of the secret d, our scheme uses y, a prime number close to n, as a modulus, whereas [GP06]'s scheme uses n. Also, instead of using basic RSA [Cor01], we use RSA-PFDH [Cor02], i.e., the signature is not computed based on the original message *msg* but on $m = H(r|msg)$ where H is collision-resistant one-way hash function and r a random value of B bits[2].

The scheme considers an RSA secret key d that is shared between $w > 2$ potential signers, whereas the corresponding RSA public key (e,n) remains private. See [Ber08] for various optimizations and recommendations regarding the choice of the parameters when implementing.
Each participant receives one share such that,

- any set of t - 1 < w shares or less, reveal no information about the secret d
- any set of t shares allows for the efficient reconstruction of d

This method, based on polynomial interpolation, is rather simple. Given any field K, a polynomial f(x) ∈ K[x] is chosen at random with a degree t - 1 and a constant term d. Next, each user $i \in U$ receives f(i) ∈ K as a share. Since each user knows a point in the polynomial, any of t users can interpolate f(x) and thus recover the secret d = f(0).

In more detail, our scheme uses the field $\mathbb{Z}_y$, with y being the closest prime to n such that $\varphi(n) < y$. Coefficients $a_1,\ldots,a_{t-1}$ are chosen randomly in $\mathbb{Z}_y$ ($a_{t-1} \neq 0$), which yields the polynomial

$$f(x) = d + \sum_{j=1}^{t-1} a_j x^j \bmod y \qquad (1)$$

If each user has an integer $i \in U$ as his or her identity and receives the share f(i) mod y, then given any number of t points $S = \{i_1,\ldots,i_t\}$, the polynomial f(x) can be interpolated based on its Lagrange form:

$$f(x) = \sum_{j=1}^{t} L_S(x, i_j) f(i_j) \bmod y \qquad (2)$$

[2] Again, see [Ber08] for the importance of H, r, and B. For instance, H prevents existential forgery and "large choices of B are often conjectured to make non-generic attacks, attacks that pay attention to the hash function H, more difficult"[Ber08]. However, none of the two enlarge the original message (msg) space and thus neither diminishes the success rate of exhaustive search.

where the Lagrange coefficients $L_S(\cdot,\cdot)$ are given by

$$L_S(\alpha,\beta) = \prod_{\gamma \in S \setminus \{\beta\}} \frac{\alpha-\gamma}{\beta-\gamma} \bmod y \qquad (3)$$

Now, each participant owns a share f(i) mod y and outputs the partial signature

$$\sigma_{m,i} = m^{f(i) \bmod y} \bmod n \qquad (4)$$

Then the altered signature $\sigma'_{m,S} = m^{d+k_S y}$ is computed by combining the partial signatures:

$$\sigma'_{m,S} = \prod_{i \in S} \sigma_{m,i}^{L_S(0,i)} \bmod n \qquad (5)$$

the RSA signature can then be obtained by removing the term $k_S y$ in the exponent of $\sigma'_{m,S}$:

$$\sigma = \sigma'_{m,S} m^{k_S y} \bmod n \qquad (6)$$

with a pre-computed $k_S = \left(d - \sum_{i \in S} L_S(0,i) f(i)\right) / y$.

3.2 The (w - 1, w)-threshold scheme

There are three types of participants: (1) The designated verifier, (2) the signer, and (3) the contributors and witnesses to the signature creation. Both the signer and the contributors will be creating a signature that the designated verifier will be able to verify. Applied to electronic voting, these participants are respectively the voter (u_2), the polling office (u_1), and the adjudicators/witnesses ($u_3,\ldots,u_w$). The witnesses are the contributors. They are trusted to cooperate with the signer (u_1 or u_2) by signing the messages they receive and by keeping their own private signing key secret.

In [GP06] the secret key would be split twice, once for each possible set of w - 1 signatories. In our scheme, the secret key is split once into w shares. k_{Sz} is computed twice, once for each set S_z with $z \in \{1,2\}$[3], where S_z denotes a set of w - 1 signatories. S_1 is the set of signatories containing the voter and all the witnesses, and S_2 is the set of signatories containing the polling office and all the witnesses. The explanations for f(x), the shares f(i), k_{S1}, and k_{S2} can be found in section 3.1.

[3] If w = 3, it is possible to imagine $z \in \{1, 2, 3\}$ since *V and P* can generate a signature without the help of the only *W*. However, this seems to have no useful application in the case of electronic voting since their interests are opposite.

It is of course possible to compute k_{Si} for each of the w subsets of w - 1 participants (out of the w potential participants), but it seems of no use when applied to e-voting, since all the other subsets would ask both the voter and the polling office to contribute to the signature. This would not contribute to the signer ambiguity concerning the two parties since both would be required to co-sign.

3.3 Instantiation of the Model

Setup $_{KGS}(\eta)$: Entering the security parameter η will generate RSA parameters MPK = (n,e,y), MSK = d.

KeyGen $_{KGS}$(MPK,MSK) : based on the RSA parameters, transmit the pair of keys (vk_i,sk_i) to user u_i where

$$vk_i = (n, e, y) \quad \forall i \in \{1, \ldots, w\}$$

$$sk_i = \begin{cases} (f(1), k_{S_2}) & \text{if } i = 1 \\ (f(2), k_{S_1}) & \text{if } i = 2 \\ f(i) & \text{if } i \notin \{1, 2\} \end{cases}$$

$Sign_{u1,W}(m,sk_1,sk_3,\ldots,sk_w)$: This is a distributed process where u_1 and $W = \{u_3 \ldots u_w\}$ collaborate in order to sign message m for the designated verifier u_2:

1. $u_1 \rightarrow u_j$: m, with $j \in \{3,\ldots,w\}$
2. $u_j \rightarrow u_1$: $\sigma_{m,uj} = m^{sk}{}_j \pmod n$ with $j \in \{3,\ldots,w\}$
3. u_1 computes $\sigma'_{m,S2} = m^{f(1)} \cdot \prod_{j=3}^{w} \sigma_{m,uj} = \sigma m^{k}{}_{S2}{}^{y} \pmod n$
4. u_1 issues signature $\sigma = \sigma'_{m,S2} m^{-k}{}_{S2}{}^{y} \pmod n$

$Sim_{u2,W}(m,sk_2,\ldots,sk_w)$: This algorithm generates a dummy signature that is indistinguishable from (in this case, identical to) the original signature returned by the algorithm *Sign*.

1. $u_2 \rightarrow u_j$: m, with $j \in \{3,\ldots,w\}$
2. $u_j \rightarrow u_2$: $\sigma_{m,uj} = m^{sk}{}_j \pmod n$ with $j \in \{3,\ldots,w\}$
3. u_2 computes $\sigma'_{m,S1} = m^{f(2)} \cdot \prod_{j=3}^{w} \sigma_{m,uj} = \sigma m^{k}{}_{S1}{}^{y} \pmod n$
4. u_2 issues signature $\sigma = \sigma'_{m,S1} m^{-k}{}_{S1}{}^{y} \pmod n$

Vrfy(σ,m,mpk) Anybody can use this algorithm to check whether σ is a valid signature on m, i.e. whether $\sigma^e = m \bmod n$.

3.4 Efficiency

This scheme is ideal. The signing-key size is bounded by the size of an RSA modulus. The signature's size is independent of the number of verifiers. In addition to the computation of a classical RSA signature by each participant, combining the w - 1 partial signatures requires only w - 1 modular multiplications. The verification process remains the same as a classical RSA-PFDH signature verification.

With y^+ and y^- as the closest prime integers to n such that $\varphi(n) < y^- < n < y^+$, if $y = y^-$ then the scheme is ideal, since each $|sk_i|$ is smaller or equal to $|n|$. However, since we know that $\varphi(n) < y^-$, this reveals some information on $\varphi(n)$. This loss of security could be avoided by choosing $y = y^+$ which produces a scheme very close to the ideal but could prevent the use of existing implementations with a fixed size for the integers.

When considering [LSMP07]'s definition of strength, where a DVS is strong if the secret key of the designated verifier is required to execute the verification algorithm, it follows that creating an MPSDVS from this threshold scheme is trivial. Indeed, the key e does not have to be public but could very well be distributed only to the designated verifier as part of his secret key. By doing so, only the designated verifier would be able to verify the designated signature using his secret key as an input to the verification algorithm.

3.5 Confidentiality

The purpose of a digital signature is not to provide confidentiality on the signed message, i.e., the purpose is not to prevent someone from recovering the message from the signature. However, this still looks like a desirable trait with regard to the witnesses and of course an external attacker.
As mentioned in section 3.1, m = H(r|msg). However a small message space could allow an adversary to perform an exhaustive search in order to determine the value of msg. In such a case, the issuer could choose m = H(r ⊕ msg) where |r| is kept secret by the issuer and is long enough to prevent such a brute force attack (possibly $|r| \gg |msg|$). The issuer also has to commit to this value by publishing H(r).
While r is revealed to W in case of conflict with the polling office, it does not leak any useful information since msg would be revealed at the same time.

4 Security

The signature-hiding property requires that the signature issued by the set of signers S_1 is indistinguishable from the signature issued by the set of signers S_2. In our case, this property is achieved since it holds that $\sigma_{m,S1} = \sigma_{m,S2} = \sigma_m$.

This section focuses on the unforgeability of the signature. The analysis is based on the simulation proof in [GHKR08].

4.1 Security against an external opponent

Let's imagine that an adversary corrupts a set of k participants, denoted $B = \{u_{i1},\ldots,u_{ik}\} \subset U$, learning all their secret information but unable to control their behaviour. That is, all users are assumed to follow the protocol.

By corrupting both u_1 and u_2, the adversary would learn both k_{S1} and k_{S2}. These values give no more information about d when taken together than when taken separately. Moreover, given our application to voting, if an attacker corrupts both the voter and the polling office, then there is little interest in securing the protocol. Therefore, the unforgeability of our scheme depends only on the security of the underlying threshold signature scheme.

As in [GHKR08], we show that the adversary, in a chosen message scenario, is unable to gain more information about the missing share than the information given by the signature σ_m itself. For this, we describe a simulator that, given only what the adversary knows, is able to generate a view of the protocol that is indistinguishable from the actual view.

Unlike previous schemes (e.g. [GHKR08, Sho00]), the Lagrange coefficients involved in our protocol can be directly evaluated, since they are computed over the field $\mathbb{Z}_y$. This makes the simulation proof much easier.

Given the simulated shares $f(i_1),\ldots,f(i_k)$ and the final signature σ_m, the simulator can directly generate a value for the missing partial signature $\sigma_{m,k+1}$ that satisfies equations (5) and (6). This can be done by interpolating $f(i_{k+1})$ in the exponent, based on the set of points $\tilde{B}= \{0,i_1,\ldots,i_k\}$, since the signature σ_m can be seen as the "partial signature" $m^{f(0)}$ of "user" 0:

$$\begin{aligned}\sigma_{m,i_{k+1}} &= m^{\sum_{j\in\tilde{B}} L_S(i_{k+1},j)f(j)} \\ &= m^{L_S(i_{k+1},0)f(0)} \prod_{j\in\tilde{B}\setminus\{0\}} m^{L_S(i_{k+1},j)f(j)} \\ &= \sigma_m^{L_S(i_{k+1},0)} \prod_{j\in\tilde{B}\setminus\{0\}} m^{L_S(i_{k+1},j)f(j)}\end{aligned}$$

The term $m^{-k_{Si}y}$, $i \in\{1,2\}$, which is required to satisfy equation (6), is simply obtained by dividing σ_m through σ'_m: $m^{-k_{S_i}y} = \sigma_m/\sigma'_m = m^d/m^{d+k_{S_i}y} \bmod n$

Therefore, the adversary is unable to gain the information about the share of the honest user necessary to forge the signature of a previously unsigned message.

4.2 Security against a dishonest participant

Even if corrupted participants do not follow the protocol, the scheme is still required to be robust. Unlike the previous subsection, this analysis takes into account the application to voting, where a distinction is made between participants according to their roles.

Dishonest Dealer

A dishonest dealer can distribute bogus shares of the key, resulting in a failure of the signature process. Moreover, the dealer could claim that the problem is due to a dishonest participant.

Protection against a dishonest dealer can also be achieved using the partial signature verification scheme described in [GRJK07], in which the dealer is required to publish the values $g^d, g^{a_1}, \ldots, g^{a_k}$ where $g \in_R \mathbb{Z}_n^*$ has a high order and $a_1, \ldots, a_k$ are the coefficients of polynomial f. Thus, participant u_i can make sure the received share f(i) is correct by verifying that

$$g^{f(i)} = g^d \prod_{j=1}^{k} g^{a_j i^j} \bmod n$$

Dishonest signers

Dishonest witnesses that output incorrect partial signatures can be detected using the verification scheme of [GRJK07]. The users are required to output the verification value gf(i) together with their partial signature σmf(i). In order to verify that the partial signature is correct, ui is asked to return xf(i) from the input x = gamb where a and b are chosen at random. Then one is able to verify that the following equality holds.

$$x^{f(i)} = \left(g^{f(i)}\right)^a \sigma_{m,i}^b \bmod n$$

It might happen that the polling office refuses to transmit the signature σ_m in exchange for the voter's ballot. It is shown in [PG99] that this problem of fair exchange cannot be solved without including an additional trusted party.

Regarding forced abstention attacks, note that in the complete scheme, a single corrupt witness should not be able to reveal whether or not a voter voted. The easiest approach would be to associate the secret share with an anonymous identity (by the use of credentials [JCJ05]) instead of the voter's real identity.

Finally, notice that the witnesses could be selected so that they have highly conflicting interests to decrease the likelihood that a coalition could form. For instance, a council involving all parties and members of the voting community (even including voters[4]) could be chosen to form the set of witnesses. With the possibility to detect malicious behavior as discussed above, it is less likely that a party would run the risk of deviating from the protocol's instructions.

5 Conclusion

The contributions of this work are threefold.

First, we showed how to provide coercion freeness from any MSDVS in e-voting (including MSSDVS, MPDVS and MPSDVS) by using them to sign the receipt created to provide verifiability.

Second, we described how to create a MPDVS and MPSDVS from any (t,w)-threshold signature by instantiating the scheme as a (w - 1,w)-threshold one.

Finally, we proposed a secure and ideal threshold RSA signature by enhancing [GP06]'s scheme and proving its security under standard assumption with a proof inspired by [Sho00, GHKR08]'s security proof. Although the scheme is ideal, due to its threshold nature, it implies an unavoidable cost in communications.

By doing so, we present a generic solution that helps create coercion-freeness in electronic voting schemes based on threshold signature schemes. We illustrate our point with an efficient, ideal, and secure threshold scheme. Compared to previous proposals, our scheme is both secure and efficient. It also leads to an easy distribution of the computations, since the partial signatures can be computed simultaneously by each participant. The scheme requires the participation of a (set of) contributor(s) to generate the desired signatures. In the framework of electronic voting, the contributor is a set of witnesses/adjudicators who help settle the possible conflicts that can occur between the polling office and the voter. Therefore, if the receipt or the signature provided by the polling office is incorrect, the voter contacts the adjudicator (the contributor) and collaborates with him or her to verify the validity of the signature together. If it appears that the voter is honest, the adjudicator can contact the polling office to resolve the problem using legal procedures when appropriate.

The number of witnesses, t- 1, can be adjusted to decrease the required trust in each of them, i.e., more distinct witnesses, each selected for their conflicting interest with the others, would have to collaborate to cheat.

[4] To reach such a high level of citizen participation, a good idea might be to divide the census in constituencies where each voter is a witness for the rest of the constituency or, as we prefer, to allow citizen to participate but to choose randomly for which constituency he will be allowed to be witness.

The scheme we present can easily be used in existing protocols based on RSA signatures in order to convert these signatures into multi-party designated verifier signatures (the existing keys can be reused as well as most of the existing software.) The scheme is being implemented in conjunction with other Internet voting and security enhancement techniques and methodology [DM11] such as Mental Booths [DL11], TreeCounting [DM10], credentials [JCJ05], or re-encryption mixnets with randomized partial checking [CH11] to provide, resistance against side-channel attacks, over-the-shoulder coercion-resistance, practical verifiability, and anonymity respectively. The implementation is available on the author's website.

Bibliography

[Ass09] Assemblée Générale des étudiants de Louvain : Election étudiante à l'ULC : une première en Belgique, 2009.

[Ber08] Bernstein, D.: RSA signatures and Rabin-Williams signatures: the state of the art, 2008.

[BG02] Boneh D.; Golle P.: Almost entirely correct mixing with applications to voting. Proc.CCS '02, pp. 68–77, 2002. ACM Press.

[BGLS03] Boneh D. et al.: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In EUROCRYPT, pp. 416–432, 2003.

[BHM08] Backes, M.; Hritcu, C.; Maffei, M: Automated verification of remote electronic voting protocols in the applied pi-calculus. 21th IEEE Symposium on Computer Security, pp. 195–209, 2008. IEEE Computer Society.

[BKS+] Baumgartner, J. et al.: Vote-auction.net.

[CH11] Clark, J.; Hengartner, U.: Internet Voting with Over-the-Shoulder Coercion-Resistance. FC 2011, vol. 2011, pp. 1–25, 2011.

[Cha96] Chaum, D.: Private signature and proof systems, 1996.

[Cho08] Chow, D.: Multi-Designated Verifiers Signatures Revisited. IJNS, 7(3):348–357, 2008.

[Cor01] Coron, J-S.: Cryptanalysis and Security Proofs for Public-key Schemes. PhD thesis, 2001.

[Cor02] Coron, J-S.: Optimal Security Proofs for PSS and other Signature Schemes. EUROCRYPT 2002, 2332:272–287, 2002.

[CV90] Chaum, D.; Van Antwerpen, H.: Undeniable signatures. Crypto'90, LNCS vol. 435, pp. 212–216. Springer, 1990.

[Des88] Desmedt, Y.: Society and group oriented cryptography: A new concept. Crypto'87, LNCS vol. 293, 120–127, 1988. Springer.

[DGB87] Desmedt, Y.; Goutier, C.; Bengio, S.: Special Uses and Abuses of the Fiat-Shamir Passport Protocol. Crypto '87, LNCS vol. 293, pp. 21–39, 1987. Springer.

[DL11] Dossogne, J.; Lafitte, F.: Mental Voting Booths, NordSec 2011, LNCS, 2011. Springer.

[DM09a] Dossogne, J.; Markowitch, O.: A Tripartite Strong Designated Verifier Scheme Based On Threshold RSA Signatures. SAM 2009, pp. 314–317, 2009. CSREA Press.

[DM09b] Dossogne, J.; Markowitch, O.: Voting With a Tripartite Designated Verifier Scheme Based On Threshold RSA Signatures. WIC09, vol. 1, pp. 113–118, 2009.

[DM10] Dossogne, J.; Markowitch, O.: E-voting : Individual verifiability of public boards made more achievable. WICSITB2010, pp. 5–10, 2010.

[DM11] Dossogne, J.; Medeiros, S. : Enhancing Cryptographic Code Against Side Channel Cryptanalysis with Aspects. WOSIS 2011, pp. 39–48, 2011. SciTePress.

[GHKR08] Gennaro, R.; et al.: Threshold RSA for Dynamic and Ad-Hoc Groups. EUROCRYPT'08, vol. 2008, pp. 88–107, 2008.
[Gol00] Goldreich, O.: Modern cryptography, probabilistic proofs and pseudorandomness, vol. 17 of Algorithms and Combinatorics. Springer, 2000.
[GP06] Ghodosi, H.; Pieprzyk, J.:. An Ideal and Robust Threshold RSA. VIETCRYPT 2006, vol. 4341 of LNCS, pp. 312–321, 2006. Springer.
[GRJK07] Gennaro, R.; et al.: Robust and Efficient Sharing of RSA Functions. J. Cryptology, 20(3):393, 2007.
[Hes02] Hess, F.: Efficient Identity Based Signature Schemes Based on Pairings. SAC'02, LNCS vol. 2595, pp. 310–324, 2002. Springer.
[HS00] Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. Eurocrypt'00), LNCS vol. 1807, pp. 539–556. Springer, 2000.
[JCJ05] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-resistant electronic elections. WPES'05, pp. 61–70, 2005. ACM Press.
[JSI96] Jakobsson, M.; Sako, K.; Impagliazzo, R.: Designated verifier proofs and their applications. Eurocrypt'96, LNCS vol. 1070, pp. 143–154. Springer, 1996.
[Lag07] Laguillaumie, F.: Multi-designated verifiers signatures: anonymity without encryption. IPL, 102(2-3):127–132, April 2007.
[LK00] Lee, B.; Kim, K.: Receipt-free electronic voting through collaboration of voter and honest verifier. JW-ISC2000, pp. 101–108, 2000.
[LSMP07] Li, Y.; et al.: Designated Verifier Signature: Definition, Framework and New Constructions. UIC'07, LNCS vol. 4611, pp. 1191–1200. Springer, 2007.
[LV04] Laguillaumie, F.; Vergnaud, D.: Multi-designated Verifiers Signatures. ICICS'04, vol. 3269 of LNCS, pp. 495–507, 2004. Springer.
[LWB05] Lipmaa, H.; Wang, G.; Bao, F.: Designated verifier signature schemes: Attacks, new security notions and a new construction. ICALP'05, LNCS vol. 3580, pp. 459–471, 2005. Springer.
[OMD04] Dall Olio, E.; Markowitch, O.:. Voting with designated verifier signature-like protocol. IADIS'04, pp. 295–301, 2004. Iadis Press.
[PG99] Pagnia, H.; Gärtner, F.: On the impossibility of fair exchange without a trusted third party. Tech. Rep., Darmstadt University of Technology, 1999.
[Pro] Proxyvote.com. Shareholder election website.
[Ric] Ricknäs, M.: Estonia to Use Mobile Phones to Simpify E-voting.
[Sha79] Shamir, A.: How to share a secret. Communications of the ACM, 22(11):612–613, 1979.
[SHCL08] Seo, S.; et al.: Identity-based universal designated multi-verifiers signature schemes. CSI, 30(5):288–295, July 2008.
[Sho00] Shoup, V.: Practical Threshold Signatures. EUROCRYPT'00, LNCS vol. 1807, pp. 207–220, 2000. Springer.
[WV10] Weldemariam, K.; Villafiorita, A.: A Survey: Electronic Voting Development and Trends. EVOTE2010, 2010.
[ZZZ08] Zhang, Y.;, Zhang, J.; Zhang. Y.: Multi-signers Strong Designated Verifier Signature Scheme. SNPD'08, pp. 324–328, 2008. IEEE Computer Society.

Session 5

Auditing and Testing of E-voting

Internet Voting System Security Auditing from System Development through Implementation: Best Practices from Electronic Voting Deployments

L. Jay Aceto[1], Michelle M. Shafer[2], Edwin B. Smith III[3], Cyrus J. Walker[2]

[1]RedPhone Corporation
9595 Sherburne Farm Road
Marshall, VA 20115, USA
jay.aceto@redphonecorporation.com

[2]Data Defenders, LLC.
10 W. 35th Street, Ste. 9F5-1
Chicago, IL 60616, USA
michelle.m.shafer@gmail.com, cyrus.walker@data-defenders.com

[3]Dominion Voting Systems
1201 18th Street
Denver, CO 80202, USA
ed.smith@dominionvoting.com

Abstract: There are many security challenges associated with the use of Internet voting solutions. While we are not advocating for the use of Internet voting in this paper, we do assert that if an Internet voting solution is going to be used, its deployment must be undertaken with continuous security auditing in place – security auditing that begins with the development of the Internet voting system by the manufacturer or election jurisdiction and continues throughout the system's use in the field.

1 Introduction

There are many security challenges associated with the use of Internet voting solutions. While we are not advocating for the use of Internet voting in this paper, we do assert that if an Internet voting solution is going to be used, its deployment must be undertaken with continuous security auditing in place – security auditing that begins with the development of the Internet voting system by the manufacturer or election jurisdiction and continues throughout the system's use in the field.

One aspect of an election security audit is real-time election forensics, which are currently being used by some election jurisdictions to monitor deployed Direct Recording Electronic (DRE) voting systems.[1] Real-time election forensics is a powerful tool in helping to prevent intrusions as well as identifying damage if a successful intrusion results. It assists the voting jurisdiction in maintaining confidence in the deployed system, and it has the advantage of being executed concurrently with the deployment, deployment testing, and use of the system.

The goal of this paper is to demonstrate how real-time election forensics and other security methodologies successfully used with electronic voting systems can also be used to mitigate risks and detect issues with Internet voting solutions.

2 Highlights of the Product Development Process

2.1 Determining What to Develop

Determining what to develop in relation to Internet voting systems requires a high degree of skill in the product management arena, higher than what is considered the norm in most product development situations, due to existing and emergent standards and threats related to Internet voting systems. The U.S. Election Assistance Commission (EAC) has published draft UOCAVA voting systems guidelines.[2] Requirements and standards published by the EAC form only one part of the requirements for any Internet voting system to be used in the United States. Each state has unique requirements when it comes to conducting elections. A voting system that is expected to be national in scope must include these requirements no matter how esoteric they may seem in statute, and the developers of that system must reconcile conflicting state requirements. Furthermore, the voting system should be able to be used by the entire population, fulfilling the needs of persons with disabilities as well as persons with literacy challenges.

Looking at the development organization, it is imperative to adopt an adaptive requirements development methodology such as the one outlined in the Capability Maturity Model Integration (CMMI) at Maturity Level 3[3]. CMMI Requirements Development, including intense surveillance for emergent information system threats, is a suitable process for deriving system requirements.

---

1 Walker, Cyrus J., *Forensics: The Vital Link in Election Integrity: A Case Study on Cook County, IL*, www.data-defenders.com/wp-content/uploads/pdfs/EIFA-casestudy-online.pdf, 2010.

2 National Institute of Standards and Technology, *High-Level Guidelines for UOCAVA Voting Systems*, www.nist.gov/itl/vote/upload/High-level-Guidelines-Draft-2011-06-21.doc, 2011-06-21 Draft.

3 Software Engineering Institute, Carnegie Mellon University, *Capability Maturity Model Integration* (CMMI) www.sei.cmu.edu/cmmi, 2012.

2.2 Determining How to Develop the System

There are a number of development methods to choose from. It does not matter so much which development method is chosen. Whether it be Waterfall[4], Agile[5], Extreme Programming (XP)[6], or some hybrid approach, all of these methods can lead to functionally secure code. There are publications that describe, independent of development method, how to write secure software[7]. What is most important is that the development method is documented, understood by developers and their management, adhered to, and auditable.

After some foundational training, the developer can be trained on the actual product architecture and the portion of the product they are developing. This same training scheme can be utilized for product testers, with additional material regarding test planning, test methods and automation, the formation of test cases, scripts, and artifacts.

2.3 Risk Management

Once the development method is chosen and the staff trained, it is not time to develop the product but rather to move into risk management for the forthcoming system. Bridging "what to develop" and "how to develop it" (the development method to be used) is the major step in system development known as risk management. Risk management, configuration management, and emergent threat management form the foundation for a robustly developed system. If this triad is not continuously functioning, there can be no secure system development or eventual deployment. Risk management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it at an acceptable level considering associated costs and benefits of any actions taken. Risk management will not preclude an adverse event from occurring; however, it enables organizations to focus on those things that are likely to bring the greatest harm, and employ approaches that are likely to mitigate or prevent those incidents. There are a number of risk management frameworks[8]. ISO 27001[9] requires that organizations adopt the standard practice of risk management with regard to management of its information security.

---

4 Waterfall Model, *Waterfall Model: Advantages, Examples, Phases and More About Software Development*, www.waterfall-model.com, 2012.

5 Poppendieck, Mary and Poppendieck, Tom, *Lean Software Development: An Agile Toolkit*, Addison-Wesley Professional; New York, 2003.

6 Beck, Kent and Andres, Cynthia: *Extreme Programming Explained: Embrace* Change (2nd Edition). Pearson Education; New Jersey, 2005.

7 Howard, Michael and LeBlanc, David, Writing *Secure Code* (Microsoft Press, 2002) is one such publication.

8 Quality Progress*, Safe and Secure: A Case Study*, Vol. 45 number 12 (Jan 2012), 16 – 23.

9 ISO 27001, ISO, Switzerland.

2.4 How to Test the System

Before considering testing the voting system and its component parts, the process used to develop the product must be audited to ensure compliance to its process documentation and to ensure that the documented process has the potential to lead to a secure voting system. This process audit approach has a parallel in-system verification and validation. Verification ensures that the product meets specification; and validation attempts to ensure that the product will work in practice.[10] The process auditor will likewise assess that the process actually employed (as seen through its artifacts) matches its governing documentation. It is likely that a larger group, such as the established or prospective customer of the system or a body such as the EAC, would seek to establish that the process has the potential of birthing a system that meets specifications and can demonstrate a required level of security.[11]

The stages of testing are well known and will not be detailed here except to provide some additions unique to an organization developing secure systems. Product testing typically starts with Unit Testing, sometimes referred to as Developer Testing. A unit is the smallest testable piece of a system[12]. Unit testing is a key activity within an Extreme Programming development environment. Code needs to be assessed during development to ensure that functionally secure code is being produced according to the established development process. Agile development methods provide for a similar outcome by requiring the developer to have work product that is usable or demonstrable after they finish the prescribed work in a given iteration of the product.

Component testing follows unit testing. This phase tests a discrete part or parts of a system – network infrastructure, firewall, and application software. Throughout these portions of the overall test program, it is useful to run static code analysis tools and to utilize other tests, likely customized for the system under development, to further ensure that the basics are being covered. "The basics" implies a code that contains no buffer overflows, dead code, poor stylistic construction, or other fundamental flaws that may or may not be uncovered through downstream functional testing. A system integration test follows to answer the question – can you conduct an election on the system? Voting systems can be developed according to the 2005 VVSG, be secure beyond imagination, and yet completely incapable of processing a jurisdiction's election.

Now that there is a nascent voting system, an intersection of process and product needs to be tested to answer the question of emergent threats. Can the development and configuration management processes manage the emergent threat environment while maintaining configuration control? This is an extremely important question to answer as

---

[10] The ISO 9000 series of standards provide definitions and uses of verification and validation in product realization processes.

[11] IEEE Standards Board, IEEE Standard for Software Unit Testing: An American National Standard, ANSI/IEEE Std 1008-1987 in IEEE Standards: Software Engineering, Volume Two: Process Standards; 1999 Edition; published by The Institute of Electrical and Electronics Engineers, Inc. Software Engineering Technical Committee of the IEEE Computer Society.

[12] Stephens, Matt and Rosenberg, Doug, *Design Driven Testing: Test Smarter, Not Harder*. Springer Science; New York, 2010.

the system moves through the remaining test phases and into deployment and use. Did the manufacturer enact appropriate policies to deal with emergent threats? Is there an adequate level of surveillance and expertise to deal with the emergent threats and transfer the needed upgrades to the product? Are these processes scalable so that the deployed system can also see the same degree of success against emergent threats that the evolving (pre-release) system enjoyed?

At a defined point in its development, that point being defined by a release process and acceptance criteria, the system begins verification testing. In a sense, verification testing has been in progress throughout the development of the product, answering the question – does the product meet the specifications, especially functional security specifications? In this phase, in contrast, the system undergoes verification as a system in an environment mimicking deployment. Verification continues to include security testing and other sorts of negative path test cases; however, most of the work at this stage will be "happy path", examining parameters such as accuracy, but not under stress or attempts to misuse the system. Validation, on the other hand, will be tied to conditions the system will face in deployment. This means adversarial testing, volume/stress testing while maintaining a secure posture and required accuracy, and enhanced accessibility and usability testing (not just line by line VVSG compliance, but sessions with a body of test subjects). While there must be bi-directional traceability from validation test cases to product requirements, the test manager will see validation activities mushroom relative to the number of activities and hours spent in unit, component, system integration, and verification testing. Significant problems during validation would likely result in re-architecture and subsequent re-development of the voting system, or possibly lead to it being scrapped in favor of an entirely new approach. The ability to develop creative test cases that test beyond conventional ways of thinking about system use is quite valuable to ensuring a secure system.

3 Security Testing of Voting Systems Methodology

3.1 Information Gathering – Internal and External Processes and Procedures

It is a well-established fact that organizations that have defined practices for their internal and external processes are less vulnerable to attack, faster to react if attacked, and forensically capable of identifying the vector of the attack (not to mention more efficient and ultimately more competitive with a higher degree of software quality assurance[13]). Organizations that clearly follow established internal and external processes are also easier for third parties to evaluate. When determining whether security vulnerabilities exist, or if and where improvements can be made that minimize vulnerabilities, having documented, established internal and external processes is vital.

[13] Capability Maturity Model Integration (CMMI), Software Engineering Institute, Carnegie Mellon. www.sei.cmu.edu/cmmi.

A quick review of the AICPA website [14] will show that process evaluation is a two-step effort; first you document and list the processes, than you evaluate them. Failure to adopt formal development and testing methodologies such as the CMMI, ISO27000 and 9000, or the Open Web Application Security Project (OWASP)[15] slows system development, causes redesign, redevelopment, failure to meet security requirements, and significantly increases the final cost of the delivered system.

Each of these methodologies has defined a process for capturing and evaluating the internal and external processes that voting system evaluators can use to uncover risks throughout the software lifecycle. It is essential that the testing effort be continuous, not a point-in-time analysis of an application's security profile. Security must be integrated early to be most successful and must be continuous to be relevant to the changing landscape of threats and vulnerabilities. Analyzing internal and external processes and requirements becomes a gap analysis between corporate processes and industry-recognized processes and best practices.

3.2 Identification and Analysis of High-level Components and Information Flow

"White hat" testing, which involves the support of the voting system manufacturer's staff up to senior leadership, is often employed. Under these circumstances, network diagrams and system component lists, including operating system versions, router Internetwork Operating System (IOS) versions, firewall logs, ports, protocols and services, etc., are demanded by testers so that an accurate inventory of all components that support the voting system exists. This is a portion of the testing and verification phase focused more on the implementation environment.

Both passive (examination) and active (testing) techniques exist for discovering devices on a network. Passive techniques use a network sniffer, such as NMAP, to monitor network traffic and record the IP addresses of the active hosts. These sniffers can report which ports are in use and which operating systems have been used on the network. Passive discovery can also identify the relationships between hosts—including which hosts communicate with each other, how frequently their communication occurs, and the type of traffic that is taking place—and is usually performed from a host on the internal network where it can monitor host communications. This is done without sending out a single probing packet. Passive discovery takes more time to gather information than active discovery, and hosts that do not send or receive traffic during the monitoring period might not be reported accurately. Both active and passive discovery have benefits and potential drawbacks but are very important to utilize.

---

[14] American Institute of CPAs, *Statements on Auditing Standards*, www.aicpa.org/Research/Standards/AuditAttest/Pages/SAS.aspx

[15] *The Open Web Application Security Project* (OWASP), www.owasp.org

3.3 Develop Misuse Cases for Violating the Assumptions

Misuse cases come within the security requirements process, which consists of (1) identifying critical assets, (2) defining security goals, (3) identifying threats, (4) identifying and analyzing risks, and (5) defining security requirements. Unlike the software development process, where the focus is on "use cases," the security testing focus is on "misuse cases," or more specifically, how to break the system and/or usurp the security and gain access to data or system administrative functions. After identifying the operating systems, manufacturer of components within the system, and internal and external processes, we look at ways we can covertly or overtly take control or alter voting data either at rest or in transit. A misuse case describes "a sequence of actions, including variants, which a system or other entity can perform, interacting with misusers of the entity and causing harm to some stakeholder if the sequence is allowed to complete." The details of use cases are usually captured in text-based forms or templates. These are important because they encourage developers to write clear, simple action sequences. The focus of misuse cases is on the disruption of any one of three primary objectives: the confidentiality, availability or integrity of the system, and supporting data. The corruption of any one will result in a system failure and lost voter confidence. Therefore, misuse cases should always be targeting one of these three security objectives.

3.4 Identification of Threats and Attack Exposures

The threat modeling process can be broken down into three high-level steps, which include decomposing the application, determining and prioritizing threats, and the identification of potential mitigations. The first step in the threat modeling process is to gain an understanding of the application and how it interacts with external entities by leveraging misuse, abuse, and use cases to understand how the application is intended to be used; identifying entry vector points to see where a potential attacker could interact with the application (voter, poll worker, or system administrator etc.); identifying assets, i.e., hardware, operating systems, internal and external processes that the attacker would be interested in, and identifying trust levels that represent the access rights the application will grant to external entities. The data flow diagram should show the different paths through the system, highlighting the privilege boundaries. Development organizations may overlook this diagram.

In the second phase, identified threats are categorized and ranked using a methodology like the NIST approach outlined in the NIST SP800-30 Risk Management Guide for Information Systems or the threat categorization methodology developed by Microsoft called STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privileges). Another very useful approach is the Application Security Framework (ASF), which defines threat categories such as auditing and logging, authentication, authorization, configuration management, data protection in storage and transit, data validation, and exception management. No matter which one is used, the goal of the threat categorization is to identify threats from both the attacker's and the defender's perspective.

Finally, countermeasures and mitigation must be examined. A lack of protection against a threat might indicate a vulnerability whose risk exposure could be mitigated with the implementation of a countermeasure. Such countermeasures can be identified using threat-countermeasure mapping lists. Once a risk ranking is assigned to the threats, it is possible to sort threats from high risk to low risk and prioritize the mitigation effort based on cost, impact, end-user use cases, etc.

3.5 Election System Threat Model Analysis

The threat model analysis for an election system indicates there are two equally potent threat sources:

- The Malicious Insider - One with malicious intentions, who developed a portion of the system and/or has been granted direct access to the deployed system. The malicious insider is the more dangerous and potent of the two threat sources.
- The Malicious Outsider - The Malicious Outsider, one with malicious intentions who attempts to gain access to the systems from outside the system operator's domain of control.

Each threat source has two main goals: minimizing exposure and maximizing impact. The means by which either threat source attempts to execute their threats against the electronic voting system depends on the state of threat model variables.

The threat opportunity for the malicious insider is generally at its peak during phase 1 and phase 2 of an election jurisdiction's election management workflow as shown in figure 1. Generally, in these phases of the election management workflow, the majority of the components of the electronic voting system are being prepared for use in an election, requiring the greatest amount of system access. As a result, a skilled and prepared malicious insider could infiltrate the system and insert foreign components, such as code, into the electronic voting system to cause it perform in a way that violates its predetermined and intended functionality.

The threat opportunity for the malicious outsider is generally at its peak during phase 3 of an election jurisdiction's election management workflow (figure 1). In this phase of the election management workflow, any publically accessible components of the electronic voting system are deployed into the field for use in an election. A skilled and prepared malicious outsider could gain access to these publically accessible components such as DREs and insert foreign components such as code into these components to cause it perform in a way that violates its predetermined and intended functionality.[16]

[16] There are a number of reports in the California Top to Bottom Review of Voting Systems from 2007. The referenced material can be found in the various source code review and red team reports from that Review. These are located at: http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm.

All these types of threats could go undetected if there are no regular checks and balances in place to validate the operational integrity of each voting system component at each step in the election management workflow.

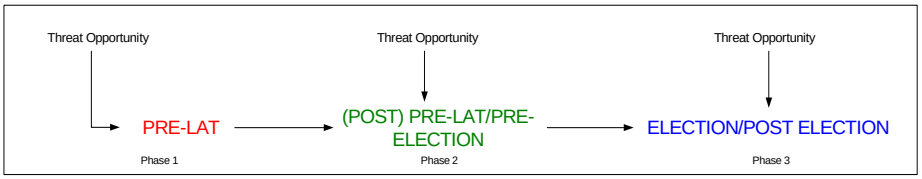


Fig. 3.: Simplistic Election Management Workflow Threat Model

4 The Importance of Election System Risk Analysis to the Forensic Auditing Process

Election system forensic auditing is a tool that can be used to mitigate the risks or operational threats against a voting system. This tool is best used when implemented as part of an overall election system risk management and mitigation strategy.

While the computer forensics process examines every part of an election system, voting secrecy is still maintained because election systems do not include voter identifiable information with ballots. The goal of the computer forensic process is to examine the election system from the bit level to detect how the smallest changes made to a system may have negative implications. It is analogous to examining the trees in a forest: once you find that out-of-place tree then you can examine the tree as well as the forest that the tree grows in. In the election system world, once a subset of data is discovered to be out of place, then the data itself can be examined as well as other characteristics, such as other occurrences of the data sample in other aspects of the systems and the impact of the data on sample on the system. The forensic auditing process can use threat modeling information as part of an operational/functional baseline for each component of the electronic voting system and incorporated threat signatures, which can be used to identify the manifestation of a threat against an election system component. This enables the most accurate validation of the operational integrity of an election system to ensure that no threats could negatively impact the operations of the electronic voting system.

Once the risk assessment has been completed, forensic auditing can be used to examine every component of the electronic voting system at the bit level, even dynamic software files heretofore considered untouchable by analytical tools. The forensic auditing process starts by developing an accurate baseline of the operations of the voting system.

4.1 Election System Baselining

System baselining is used to establish a functional benchmark of a system that can then be used to measure and determine the operational integrity of the system during actual use. The system baselining process can be used to establish functional benchmarks of DRE-based or Internet-based voting system. A typical system baseline consists of the following components:

- File System Structure
- Static and Dynamic File Delineation
- Dynamic File Range of Change
- Identified System State Transition

While not every function or capability of a static file is executed during routine system operations, the static file itself will not change at any time during routine system operations unless some other program function legitimately caused it to change, for example, program or system updates. Therefore, the behavior of a static file is limited and can easily be characterized.

Dynamic files are designed to change based on routine system operations. The presence of dynamic files should not be intimidating as, generally, the range of change of the dynamic file is limited and based on the routine system operation, which is limited, and as such, the range of change can be defined and measured. Log files are considered dynamic in practice and under the EAC definition can be found in VVSG 2005, Volume I, section 7.4.

One threat common to all system models is the threat against dynamic files. Because dynamic files are generally designed to change during normal routine system operation, if a malicious change is made to a dynamic file, that change would be difficult to identify unless the expected changes of a dynamic file have been delineated and used to validate actual changes made to dynamic files during routine system use.

File behavior is limited based on the limited set of routine system operations; thus, file behavior can be measured, captured, and used to validate future file behavior measurements to determine if those measurements are based on legitimate or malicious system activities.

4.2 Forensic Auditing Process Implementation

Forensic auditing is not about trust or the lack thereof; it is about validation. The only way to absolutely guarantee the operational integrity of a system is to completely eliminate all access to the system. That is clearly not feasible. Therefore, if there is any access to the system, validation of the operational integrity must also be executed to ensure that the operational integrity of the system.

One valuable benefit of forensic auditing is that no component of the forensic auditing process needs to be installed on any component of the electronic voting system during the audit process.

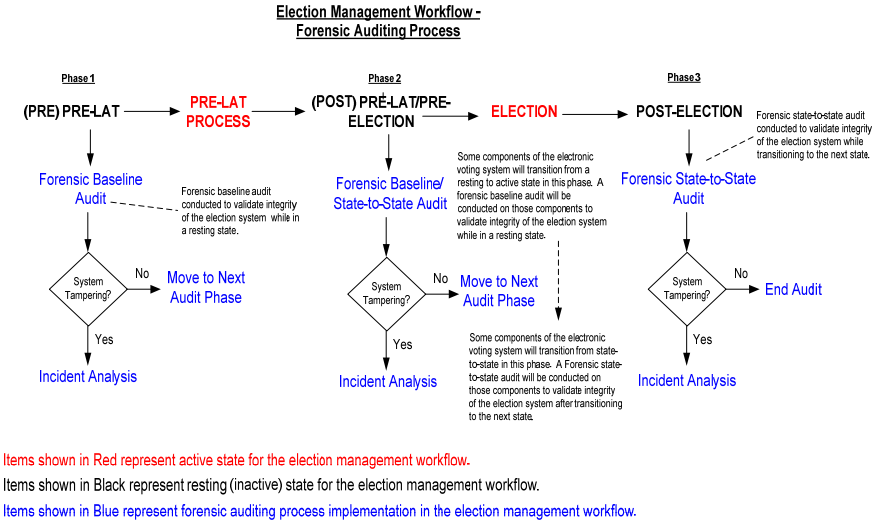


Fig. 4.: Election Management Workflow & Forensic Auditing Process

The election management workflow is cyclical: the electronic voting system usage is commensurately cyclical. There are significant periods of time where the election system is not used and simply awaiting the next election cycle.

The process of forensic auditing consists of taking samples of data from target electronic voting system components at various intervals in the election management process. Each data sample collected is analyzed by comparing that sample of data to a "known good state" of data contained in that sample, in order to identify and validate the integrity of changes made to that data sample as a result of normal, routine system operations or to identify anomalies (unexpected changes) in the data sample made by foreign code or components inserted into the system, which both have the effect of negatively impacting the operational integrity of the electronic voting system.

"Known Good States" are data samples that have been taken from a number of sources including election system manufacturers, Voting System Test Laboratories (VSTLs), and data samples from a clean, unused state of the target system. Each clean sample of data is assembled into a single "Known Good State" baseline for the target device and used to validate the integrity of the data samples taken from that device during a forensic audit. Analyzing each data sample consists of conducting a "Resting State" to "Baseline" comparison or a "State-to-State" comparison to identify and validate changes made in the data sample.

General computer forensic methods such as acquiring data samples and generating hash values for that data, are used to ensure that the integrity of the data sample is maintained and can be validated at any point in the analysis process. This ensures that none of the analytic processes made changes to the data sample, which could lead to inaccurate results. The goal of the analysis is to validate that known static files were unchanged and that the changes made to dynamic files were valid and according to forensic audit expectations.

When forensic auditing is used and implemented in the manner previously described, it can serve as a detection function, detecting if the operational integrity of the electronic voting system has been impacted in any way. Additionally, with the forensic auditing function being regularly executed on the electronic voting system, it serves to deter the malicious insider as a result of its recurring implementation.

5 Conclusion

Designing security into the Internet voting system is extremely important. A suitable methodology includes internal and third party assessment of risk management competency, development and test process documentation, and adherence to that documentation. The development and deployment team for Internet voting must have a superior system for recognizing, assessing, and managing emergent threats to the voting system.

Process and product (voting system) auditing alongside continuous, multi-pronged testing from the development stages through implementation is critical for any voting system – prior to, during, and after each voting system use.

Forensics must be used before and during system deployment to identify intruders, aid in stopping their malicious efforts, and delineating any damage a successful intrusion might have caused.

These efforts, product and process auditing, unit through system testing, and forensic analysis are being utilized on hardware-based electronic voting systems, and we assert that these same methodologies will assist in guarding against and detecting security issues associated with internet voting systems.

Bibliography

[Epp12] Dana Epp, Microsoft MVP Enterprise and Developer Security, "The Evolution of Elevation: Threat Modeling in a Microsoft World", 2012. http://technet.microsoft.com/en-us/security/hh778966.aspx

[Sin05] Sindre, G and Opdahl, A. L., *Eliciting Security Requirements with Misuse Cases*. Requirements Engineering Journal, 10(1):34–44, 2005.

[Wal11] Walker, Cyrus J., *A Case Study of Real-Time Election Forensics,* Data Defenders, 2011. www.data-defenders.com/wp-content/uploads/2011/07/A-Case-Study-of-Real-time-Election-Forensics-FINAL.pdf

Testing Democracy: How Independent Testing of E-Voting Systems Safeguards Electoral Integrity

Mark D. Phillips
President, SLI Global Solutions
216 16th Street
Denver, Colorado 80202 USA
mphillips@sliglobalsolutions.com

Richard W. Soudriette
President, Center for Diplomacy and Democracy
3430 Clubhouse Court
Colorado Springs, Colorado 80906 USA
soudriette@aol.com

Abstract: When properly implemented, electronic election systems provide accurate vote counting, timely transmission of results, and secure electoral processes. Independent testing and certification by qualified testing laboratories offer election administrators, election stakeholders, and the public assurance that e-voting systems are trustworthy. Testing is an essential tool to safeguard the integrity of e-voting systems.

1 Introduction

In 1892, the lever voting machine was used for the first time in Lockport, New York. The inventor, Jacob H. Myers said that his invention would

> "*protect mechanically the voter from rascaldom, and make the process of casting the ballot perfectly plain, simple and secret."*[1]

While most electoral democracies still rely on traditional paper ballots and ballot boxes for their elections, over the past 20 years many countries have turned to e-voting technologies. E-voting systems have been implemented with a range of technologies including direct recording devices, optical scanning systems, and a variety of Internet-based systems, all of which capture, transmit, consolidate, count, and report election

[1] This notation was cited in Dr. Douglas W. Jones's book titled, "A Brief Illustrated History of Voting," (University of Iowa 2001), Chapter 6.

results. When implemented properly, e-voting can protect the rights of voters and safeguard electoral integrity.

Independent testing and certification of e-voting systems are essential tools that election management bodies (EMBs) should use to guarantee the performance of e-voting systems and to promote public confidence. Transparency in both testing and certifying e-voting systems also promotes credibility among election stakeholders such as political parties, the media, and civil society. This paper will discuss the following aspects of testing and certification:

- Technology challenges faced by election administrators
- Need for international election testing standards
- Review of current e-voting hardware/software testing methodologies
- Case studies in election testing and certification
- Impact of independent testing and certification on electoral integrity

If e-voting systems are in use, it is imperative conduct both internal and independent testing to ensure that e-voting systems are functioning correctly and accurately. The infamous "punch card voting machines" and "hanging chads" of Florida from the cliffhanger U.S. presidential election in 2000 demonstrated that the lack of adequate testing and maintenance of voting equipment undermines voters' faith in the democratic process.

Election administrators who are considering implementing an e-voting or Internet voting solution should include adequate funding for the independent testing and certification of such voting systems. In 2010, the Commission on Elections (COMELEC) in the Philippines held fully-automated, nationwide elections. Overall, the election was viewed as a success in the eyes of the voters, who were pleased to know the winner of the presidential elections 48 hours after the closing of the polls. A key to the successful use of voting equipment was a robust independent testing and certification program.

2 Technology Challenges Faced by Election Administrators

Despite the potential advantages of e-voting systems, many election officials are reluctant to embrace automation at the polls. This hesitance is fueled by increased opposition to new voting technologies. In countries where e-voting is in use or being considered, election administrators face resistance by opponents of e-voting technology in all its form. Many election technology foes strongly believe that legitimate elections can only be conducted with traditional paper ballots, ballot boxes, and tabulation of election results by hand.

In the U.S., opponents of direct recording electronic (DRE) machines have been successful in convincing officials at all levels of government of the unreliability of DREs and the need to add printing capabilities to existing machines to produce a paper trail of each recorded vote. This insistence on having a Voter Verified Paper Audit Trail (VVPAT) has added major costs to state and local elections.

Since the passage of the Help America Vote Act in 2002, there have been a handful of lawmakers in the U.S. Congress who have introduced legislation that would mandate a return to the use of traditional paper ballots. In 2008, two U.S. Senators introduced legislation that would have completely banned the use of touch screen DRE machines for the U.S. presidential election in 2012. While none of these measures have passed in Congress, they do help to undermine the credibility of e-voting as well as the election process.

In Europe, the anti-technology backlash has virtually halted the use of e-voting systems: The Dutch had been pioneers in the use of voting technology since the late 1960s, until a dramatic shift occurred in 2008 when anti-technology Dutch activists forced the Dutch Government to scrap nationwide use of DRE machines in elections.

Over the past decade, the U.K. has experimented with e-voting technology for pilot elections for local and E.U. parliamentary elections. At the present time, however, it appears that there is little enthusiasm nationwide for embracing new voting technologies. The only bright spot for election technology is in London, where an e-counting system was used for local elections in 2008 and will be used again in 2012.

Belgium is one of the few exceptions in Europe, having decided to use a DRE voting system on a limited basis in municipal elections in 2012.

3 Need for International Election Testing Standards

To reverse the anti-technology trend in elections, EMBs should rely on independent testing and certification of e-voting systems. Presently there are no internationally recognized standards that mandate the conduct of election technology testing and certification. However, there are initiatives that are taking place in several countries.

The Council of Europe established a basic set of standards governing e-voting in 2004. These standards emphasize the need for reliable auditing of voting systems as well as certification. Yet there are no specific protocols or procedures governing independent testing and certification of e-voting systems. In 2010, the Council of Europe released an excellent publication, *The E-Voting Handbook*, which encourages the independent testing and certification of e-voting systems.

In the U.S., extensive testing and certification of voting systems is in place for both e-voting and Internet voting. The U.S. Election Assistance Commission (EAC) oversees the testing of voting systems in cooperation with the National Institute of Standards and

Technology (NIST) and is responsible for accrediting Voting Systems Test Laboratories (VSTL). Generally, when states and municipalities use federal funds to buy voting equipment, the equipment is certified by accredited VSTLs. The EAC mandates that equipment testing be conducted independently and without interference from vendors.

VSTLs test voting systems using a set of criteria developed by the EAC called the Voluntary Voting Systems Guidelines (VVSG). Most states follow the EAC guidelines and protocols. However, several states such as New York, California, and Ohio have either amended these requirements or have developed their own election testing standards and certification programs. The New York State Board of Elections concluded an extensive election testing and certification program in 2009 which helped to replace antiquated voting equipment across the state.

One way to expand the use of e-voting would be for international election experts and institutions to work together to develop a basic set of testing and certification standards. Some of the groups that might take the lead in such an effort include the United Nations Development Program, Association of European Election Officials, E-Voting CC, Carter Center, International Foundation for Electoral Systems, Electoral Institute of Southern Africa, and the OSCE Office for Democratic Initiatives and Human Rights.

4 Review of Current E-voting Hardware/Software Testing Methods

Testing and certification should be undertaken to verify the accuracy, reliability, and security of e-voting systems. Since 2003, the EAC has awarded more than USD$2 billion in federal funds to states and municipalities to upgrade their voting systems. Independent testing and certification of voting equipment help demonstrate that taxpayers' money is being well spent on reliable voting systems.

In 2006, the Carter Center reported on the Venezuelan presidential elections and stated:

"Impartial, independent, and transparent system certification measures should be in place to insure that the system meets national or international standards, the requirements of the election's jurisdiction, as well as the technological specifications outlined by the vendor."[2]

[2] See Carter Center's report on the Venezuelan Elections in 2006 entitled, *Developing a Methodology for Observing Electronic Voting,* page 6.

The major e-voting tests currently used by independent laboratories include:

- Acceptance Testing: Testing the functionality of software used in e-voting systems
- Performance Testing: Testing of performance and speed of hardware and software
- Stress Testing: Testing the endurance of voting systems even under extreme conditions
- Security Testing: Testing for data protection and functionality of e-voting systems
- Usability Testing: Testing for voter-friendly e-voting systems
- Trusted Build: E-voting systems are rebuilt under controlled conditions using the vendor specifications to insure they function properly
- Source Code Review: Systematic testing of source code for e-voting systems.[3]

EMBs that are considering automating voting systems are advised to engage in sufficient analysis and planning prior to moving to the procurement phase. Poor implementation of e-voting systems can result in costly errors both in terms of public finances and public confidence.

The Republic of Ireland learned a tough lesson following the botched implementation of e-voting in 2004. The decision to replace traditional paper ballots with a DRE system ultimately cost Irish taxpayers approximately €55 million and a loss of electoral credibility. This ill-fated e-voting scheme was conceived by government bureaucrats with little public input from the election stakeholders. The DRE system was scrapped before it was ever used and this fiasco resulted in a major setback for e-voting across Europe. Adequate planning, thoughtful procurement, and independent testing would have produced better results.

In Ben Goldsmith's recent book *Electronic Voting & Counting Technologies* he makes the case for having sufficient lead time and preparation when EMBs modernize voting systems. This includes feasibility studies and pilot elections prior to nationwide implementation: *"Once delivered, it is essential that an EMB ensure that an electronic voting or counting system not only meets the specifications developed for the system, but also meets the requirements of the electoral environment."*[4] The best way to ensure that voting systems perform as intended is to independently test and certify the systems prior to an election.

---

[3] See The Council of Europe Handbook for E-Voting, pages 34-35.

[4] See Ben Goldsmith's, "Electronic Voting & Counting Technologies--A Guide to Conducting Feasibility Studies," page 6.

5 Factors to Consider for Successful Testing and Certification

Independent testing must combine absolute objectivity, the highest ethical standards, and proven testing methodology. Also, test laboratories must be able to work closely with EMBs and stakeholders to engender maximum public confidence in the electronic election system.

Objective accreditation is vital for the testing, auditing, and certification of e-voting systems. The International Standards Organization (ISO) recognizes the effectiveness of testing facilities by awarding its coveted designation *ISO: 9001:2008.* Also, ISO uses the internationally recognized test standard known as *ISO-17025* to gauge the capacity of testing labs to fully replicate and audit test results as an indicator of testing competence. In the U.S., the National Voluntary Laboratory Accreditation Program of the National Institute of Standards and Technology as well as the EAC, engage in accrediting election test laboratories. These types of accreditations are useful because they provide EMBs with confidence that the testing methodologies used by test labs are reliable, repeatable, and objectively verifiable.

Voting systems have unique demands. For example, optical scan counting systems must be able to accurately and reliably read the hand written marks of voters as they indicate their candidate preferences on paper ballots. If not properly designed and tested, the variability in handwriting of the voters can impact the performance of scanning systems and may even potentially impact the accuracy of the vote count. Most generalized software testing labs have experience in code and process review but may lack specific methodology and techniques to ensure that electronic election systems operate as required. Test methods must be configured in a way to ensure the effective validation of voting systems that fully comply with the electoral law as well as the requirements of EMBs. Testing labs need to demonstrate that they stand behind their work and that they have extensive automated management, repository, and reporting tools necessary to guarantee that e-voting systems will report election results with transparency and accuracy.

Experience with a broad range of electronic election systems is important to design effective tests and provide accurate as well as timely test results. As voting systems, ballot designs, and election processes vary worldwide, it is crucial to understand how these differences can impact electronic voting. The variety of election management systems poses logistical challenges and may reveal vulnerabilities of e-voting systems. These potential weaknesses will certainly be exploited by anti-technology activists as they seek to derail the use of e-voting, which is why independent testing is so essential. Direct experience with election testing can also help EMBs better understand the importance of properly communicating test results to election stakeholders with divergent points of view such as political parties, civil society, and the media.

6 Case Studies in Election Testing and Certification

Since no international testing standards governing independent testing and certification of e-voting systems exist, it is useful to consider how EMBs currently using e-voting systems are dealing with this issue.

E-voting in Brazil began in the late 1980s. By 1996, the Supreme Electoral Tribunal of Brazil introduced e-voting nationwide for federal elections. The Tribunal has long understood the importance of adequate testing of voting machines in use. They have accomplished this through internal testing done by Tribunal's staff and independent testing conducted by the Brazilian National Institute of Space Research. Several scientists from this agency were involved in the original design of the Brazilian DRE machine.

The U.K. has been reluctant to move forward with full implementation of e-voting and e-counting systems. From 2000 to 2007, the U.K. Government supported many pilot elections around the country using a wide variety of voting technologies. Under current U.K. law, e-voting can only be used for local and EU parliamentary elections.[5] Only traditional paper ballots may be used for U.K. parliamentary elections. Intense public pressure by anti-technology activists forced the government and the U.K. Electoral Commission to temporarily suspend support for pilot schemes using e-voting technology. Using local financial resources, the one exception has been the Greater London Authority (GLA), which authorized and funded the use of an e-counting system for the municipal elections in London in 2008 and in 2012. The GLA made independent testing and certification a priority in both elections.

In 2004, the Electoral Commission of India (ECI) took a leading role in the use of e-voting technology. The ECI introduced the Electronic Voting Machine (EVM) which was successfully used in nationwide parliamentary elections in 2004 and 2009. While testing does play a role in the work of the ECI, it is done internally by the Electoral Commission and by the EVM manufacturer. Due to increased concerns by election stakeholders during the 2009 elections, the ECI invited critics to share specific information about perceived or actual vulnerabilities in the EVM system. For the most part, the 2009 parliamentary elections went smoothly. However, the ECI has recently shown interest in independent testing for future elections.

One of the cornerstones of the plan to enhance democratic institutions in the Philippines was the introduction of electronic devices to count votes and transmit election results more quickly and accurately. According to the former Chief Justice of the Supreme Court of the Philippines, Reynato Puno, *"Full automation will not completely cleanse the dirt in our electoral system, but it is a big leap forward which can lead us to the gateway of real democracy where the vote of the people is sacred and supreme."*[6]

---

[5] See August 2007 Bulletin of the Electoral Commission of the U.K. entitled, "Key Issues and Conclusions-Electoral Pilot Schemes."

[6] See interview on GMA TV News broadcast interview on September 11, 2009 with former Chief Justice Reynato Puno of the Philippines.

To accomplish this goal, COMELEC of the Philippines successfully implemented the use of 80,000 precinct count optical scan (PCOS) machines. Planning for implementation of the new automated voting system started in 2008; two years before the election. When COMELEC developed their automation plan they included independent testing and certification as major program components. Because COMELEC was unable to find international voting systems guidelines, the decision was made to adapt portions of the Voluntary Voting Systems Guidelines of the EAC and then combine these specifications with additional Philippine statutory requirements.

COMELEC was especially determined that the 2010 elections be well received by the public, so they made certain that independent testing and certification were key components of their automation efforts. With the help of independent testing, COMELEC was able to resolve design problems and ensure that the vendor delivered the PCOS machines on schedule. The testing and certification also enabled COMELEC to promote confidence in the new system among voters, political parties, civil society, and the media. Election administrators contemplating the use of e-voting should carefully study the case of the Philippines.[7]

The election testing and certification system in the U.S. has evolved over three decades. The U.S. Federal Election Commission (FEC) made initial efforts to establish early standards for e-voting systems in the U.S. Later, the National Association of State Election Directors launched a voluntary testing and certification program for voting systems that has evolved into the current system overseen by EAC and NIST.

The passage of the Help America Vote Act in 2002 created the EAC. One of the mandates of the EAC was to assume oversight of voting systems standards and testing. Congress gave the EAC the authority to disburse nearly USD$3 billion in federal funds to state and local election officials to replace antiquated voting systems such as the punch card voting machines in states such as Florida, Illinois, and Ohio. EAC funds have been used to purchase voting systems that were certified by the EAC accredited testing laboratories. Currently the terms of all of the EAC commissioners have expired, and it is doubtful that any new commissioners will be named by 2013 at the earliest. Nevertheless, the testing program, protocols, and procedures of the EAC are still in force.

[7] See article by Richard W. Soudriette, "Philippines Test E-Voting," *Modern Democracy,* page 3, February 21, 2011.

A major issue faced by election administrators is the security of the source code for e-voting systems. This became the hot button issue in the Philippines prior to the 2010 elections. The review of the source code is a critical element in the testing and certification process. Many opponents of the automated voting system in the Philippines were fearful that the source code could be manipulated to rig the election, or that corrupt elements would penetrate the security of the software for the purpose of corrupting the election results. Because of this concern the COMELEC, using its independent third-party testing lab, conducted an extensive review of the source code for the PCOS machines and provided controlled access to political parties and NGOs to examine the results.

Other electoral management bodies such as the Supreme Electoral Tribunal of Brazil and the New York State Board of Elections have also made source code accessible to parties, civil society and the public. In offering this access it is vital that election officials safeguard the sanctity of e-voting systems by not actually allowing the source code to be downloaded for the purpose of conducting off site testing and review. EMBs must guard against tampering with the code in an uncontrolled environment. Another issue related to source code is that election management bodies may face difficulty getting full access to the code from the equipment vendors due to intellectual property issues. When entering into vendor contracts, election administrators should ensure that the contract language grants EMBs full access to the source code. To protect intellectual property rights, the vendors may require election administrators to sign confidentiality agreements to eliminate the fear that corporate secrets will be tapped by competitors.The use of Internet voting is increasingly seen as an important tool by election administrators. For the elections in 2012 in Mexico City, the election authorities plan to use Internet voting to permit out-of-country voting. In 2011, the Norwegian Ministry of Local Government and Regional Development conducted pilot local elections in 10 municipalities using Internet voting. The OSCE/ODHIR election team that observed these pilot elections noted that, for the most part, the pilot elections were successful. More than 27,000 voters cast their ballots via the Internet. In their report, the OSCE/ODHIR observer team stated that some voters experienced difficulty using the Internet voting system. The same report mentioned a lack of adequate auditing and certification of the internet voting system.[8]

Critics of Internet voting have pointed out that limited pilot projects, such as the one in Norway, do not adequately reflect the threats that could occur in larger elections. Threats including denial of service (DOS), DNS routing manipulations, and the generally uncontrolled environment of the Internet are cited as being more attractive to persons with malicious intent as the stakes and visibility of elections increase. Proponents point out the convenience and improvements in citizen participation promised by properly implemented Internet solutions. Given the open nature of Internet solutions that may permit voting anytime, anywhere, and regardless of device, it is necessary to have trusted third party penetration, testing, vulnerability testing, code review, and security audits of the voting servers to ensure a strong defense for any Internet voting system.

[8] OSCE/ODHIR election reports regarding Norway can be found at http://osce.org/odhir/elections/norway.

7 Impact of Testing and Certification on Electoral Integrity

Election administrators often view e-voting systems as a panacea to resolve all election problems. E-voting is merely a tool, not a replacement for competent and professional election administration.

In the Republic of Georgia in 2004, some politicians viewed the Central Election Commission (CEC) with disdain and suspicion. A bill was introduced to replace the CEC with e-voting. That same year the International Foundation for Electoral System invited the Deputy Speaker of the Georgian Parliament and several of his colleagues to observe elections in the U.S. They visited many American polling stations using a variety of e-voting systems. Their overall observation was that the key to good elections lies not in the voting equipment but in the work of election administrators.

Automation of voting systems can represent a major investment of public funds. The budget for the development and operation of the automated voting system in the Philippines for the 2010 election was about USD$150 million. While this is a substantial investment, the e-counting system used in the Philippines accurately recorded, consolidated, and reported the votes of over 50 million Filipinos within hours of the close of the polls. The 2010 elections stood in contrast with the previous elections when voters had to wait for days, weeks, and months before election winners and losers were known. Additionally, the e-counting system has the potential of holding down costs if used for future elections.

On the issue of e-voting systems and potential cost savings, the experience of Mexico should be noted. Since 2008, the Electoral Institute for Citizen Participation – *Instituto Electoral de Participación Ciudadana* (IEPC) of the state of Jalisco has systematically developed an e-voting system through phased implementation. IEPC has found that while initial development and deployment costs of e-voting systems are high, the long-term use of e-voting systems is cost effective.[9]

Given the high initial cost of voting equipment, a number of steps should be taken before the green light is given to purchase e-voting equipment. These steps include feasibility studies, pilot elections, open procurement processes, independent testing and certification, and effective outreach to election stakeholders to inform them of every step in the process. Given the considerable opposition to e-voting technology worldwide, it is a duty incumbent upon election administrators to procure e-voting systems that are voter friendly, accurate, and secure. An independent testing and certification program should be an essential part of the selection and procurement process to ensure that the system operates as promised on election day.

[9] See the 2011 report of the IEPC of Jalisco entitled "Proyecto Urna Electrónica de Jalisco."

In countries accustomed to contentious elections, the lack of adequate testing of e-voting systems can undermine democracy. Independent testing in 2010 helped COMELEC diffuse concerns about the potential for manipulation of the Philippine elections. By keeping election stakeholders informed about the testing and certification process, COMELEC was able to maintain public confidence in the new election system.

8 Conclusion

Election administrators face a small but vocal group of anti-election technology opponents. While some EMBs may not wish to automate their electoral processes, e-voting holds great potential as a valuable tool in the advancement of democratic rights.

For successful implementation of e-voting, independent testing and certification programs should be required. By embracing testing as an essential tool, election officials can ensure that the e-voting systems they procure have the best possible chance of operating flawlessly on election day. Testing and certification can also reassure citizens, candidates, and election stakeholders about the transparency and accuracy of e-voting.

The best assistance that the international election community can provide to expand the reach of e-voting is to work toward the development of international standards and protocols governing the independent testing and certification of e-voting systems. Enlisting the support of international and regional election organizations in the development of international voluntary voting systems guidelines would also be a major advancement in the field of election administration.

When properly implemented, electronic election systems count quickly and accurately. E-voting systems make the voting process more accessible and speed up the release of accurate election results. There are many examples worldwide where the slow release of election results has increased public anxiety and sparked civil unrest. If voters have confidence in the credibility of e-voting machines, they will trust the results. Independent testing and certification of e-voting systems are vital tools to safeguard the sanctity of the ballot box and the integrity of the democratic election process.

Glossary of Acronyms

COMELEC	Commission on Elections of the Philippines
DRE	Direct Recording Electronic Machine
EAC	Election Assistance Commission (USA)
ECI	Electoral Commission of India
EMB	Electoral Management Body
EVM	Electronic Voting Machine (India)
FEC	Federal Electoral Commission (USA)
GLA	Greater London Authority
HAVA	Help America Vote Act

IEPC	Electoral Institute for Citizen Participation – *Instituto Electoral de Participación Ciudadana* of Jalisco, México
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
OSCE/ODHIR	Organization for Security and Cooperation in Europe/ Office of Democratic Institutions and Human Rights
PCOS	Precinct Count Optical Scanner
VSTL	Voting Systems Testing Laboratory
VVPAT	Voter Verified Paper Audit Trail
VVSG	Voluntary Voting Systems Guidelines

Bibliography

[Ca06] Carter Center. Developing a Methodology for Observing Electronic Voting. Atlanta 2006.

[Co10] Council of Europe. Handbook for E-Voting. Brussels 2010.

[El11] Election Assistance Commission (USA). Voting System Testing and Certification Program Manual..Washington, D.C. 2011.

[El05] Election Assistance Commission (USA). Voluntary Voting Systems Guidelines-Vol. I & II. Washington, D.C. 2005.

[El07] Electoral Commission of the U.K. Key Issues and Conclusions—Electoral Pilot Schemes," EC Bulletin, August 2007.

[Go11] Goldsmith, Ben. Electronic Voting & Counting Technologies—A Guide to Conducting Feasibility Studies. Washington, D.C.: IFES 2011.

[Go05] Government and Accountability Office (USA). Elections—Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Underway but Key Activities Need to Be Completed. Washington, D. C. 2005.

[Jo01] Jones, Douglas W. A Brief Illustrated History of Voting. Des Moines: University of Iowa 2001.

[Os11] OSCE/ODHIR. Norway Internet Voting Pilot Project - Local Government Elections on 12 September 2011- Election Expert Team Report. Warsaw 2011.

[Sa06] Saltman, Roy. Independent Verification: Essential Action to Assure Integrity in the Voting Process .Gaithersburg, MD: National Institute of Standards and Technology 2006.

[So11] Soudriette, Richard W. "Philippines Test E-Voting," Modern Democracy, February 21, 2011.

[Sw09] Swamy, Subramanian. "Are Electronic Voting Machines Tamperproof?" The Hindu. June 17, 2009.

[Ya10] Yard, Michael. Ed. Direct Democracy: Progress and Pitfalls of Election Technology. Washington, D.C.: IFES 2010.

Session 6

Practical Experience with Internet Voting

E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons

Ardita Driza-Maurer, Oliver Spycher, Geo Taglioni and Anina Weber

Federal Chancellery,
Section for Political Rights,
Bundeshaus West, 3003 Bern, Switzerland
{ardita.driza-maurer | oliver.spycher | geo.taglioni | anina.weber}@bk.admin.ch

Abstract: The ever-increasing number of expatriates has fed the political debate on the voting rights of Swiss abroad over the last two decades. More than the right to vote itself, the effective exercise of voting rights has become a much-discussed issue. Swiss expatriates are able to vote at the federal level, which means they are invited to vote in popular votes and referendums up to four times a year and in elections every four years. They vote mainly by post and are faced with delays inherent to this method of voting and are sometimes disenfranchised as a result. Internet voting considerably accelerates the return of the ballot. Its introduction has been one of the main demands of Swiss living abroad. In parallel, the federal and cantonal authorities have planned to gradually and pragmatically adapt direct democracy instruments and voting methods to the digital environment in a prudent and long-term process. Internet voting was launched at the beginning of the 21st century and is one of the key projects of the Confederation's e-government strategy. Three Internet voting systems have been developed so far by the cantons of Zurich, Neuchâtel, and Geneva. Internet voting was first offered to Swiss expats in June 2008. For the latest federal elections on February 13, 2011, some 55,000 Swiss abroad had the possibility to vote via Internet; on the federal elections on October 23, 2011, some 22,000 Swiss abroad registered in four cantons took part in the very first Internet voting trial during a federal election. Half of Swiss cantons have now introduced Internet voting, mainly for citizens abroad. While it is too early to draw conclusions on whether Internet voting fosters participation of expatriates in Swiss political life, recent experience clearly shows that Internet voting is well accepted. The success of the Swiss model of the introduction of e-voting can be explained with the following elements: joint strategic planning (the roadmap), a good inter-cantonal cooperation with hosting solutions, and a gradual expansion, which puts security at the center of efforts.

1 Introduction

Switzerland has a long tradition of citizen participation in the decision-making process at federal, cantonal, and local level. In addition to elections, which are held every four years, direct democracy instruments such as referendums[1] and initiatives[2] at all levels, and the ensuing high frequency of votes[3], encourage citizens to take part in the democratic process. Voting methods have traditionally adapted to take account of voters' needs and social developments and are broadly considered to be citizen-friendly. They evolved from the people's assembly[4], to voting at the polling station, to postal voting, and finally to Internet voting (also referred to as e-voting), not to forget a short foray into SMS-voting[5]. A distinctive feature is the co-existence of several voting methods; at least two are always available in every canton: voting at the polling station and voting by post[6]. Completely liberalized postal voting – also a sort of remote voting – is one of the main features of Swiss voting procedures. Family voting is not an issue in Switzerland during the public debates, not even in discussions on postal voting. Remote or distance voting from an uncontrolled environment (typically home) on the Internet has been tested and introduced on a limited scale and in a controlled manner since the beginning of the 2000s. It is currently being used by half of the 26 cantons[7] that constitute the Swiss Confederation. Most of them initially offered e-voting to their citizens living abroad[8].

The relatively short deadlines to mail the voting material (ballot papers) for federal elections combined with problems in terms of postal delivery and the postal system in various countries meant that Swiss voters living abroad risk being disenfranchised. The deadlines for mailing voting material for federal elections are more generous than for other elections, so the potential for problems regarding disenfranchisement is lower. The observers of the Organisation for Security and Cooperation in Europe (OSCE/ODIHR) present at the federal elections in 2007 identified problems with the issuing of voting

1 At the federal level it's a popular vote on Federal Assembly legislation, total or partial revision of the federal Constitution, international treaties, or agreements on accession to international organizations.

2 Generic term for various procedures by which a pre-determined minimum number of Swiss citizens who are eligible to vote may make a request in terms of a general proposal, an amendment be made to the Constitution, or by which a canton or any member of the Federal Assembly, parliamentary group, or committee proposes a Federal Assembly bill or the fundamental elements of such a bill.

3 Up to four times a year a federal vote is organised on referendums or initiatives that have obtained the required number of signatures. Federal elections are held every four years.

4 This traditional, public voting method involving a show of hands is still practised at cantonal level in a few cantons. It is widely used at the local level by many communes. The *Landsgemeinde* voting channel is not permitted for federal votes.

5 Canton Zurich (ZH) trialed code-voting via SMS until 2008.

6 With the exception of the canton Ticino, where postal voting is only available for federal elections and votes, all other cantons allow postal voting at local, cantonal and federal level.

7 The 26 cantons of Switzerland are the member states of the federal state of Switzerland.

8 Swiss abroad are considered to be all Swiss people who have no residence in Switzerland (Art.2 of the Federal Act on Political Rights of Swiss Abroad, SR 161.5 http://www.admin.ch/ch/f/rs/c161_5.html). The Federal Act on Swiss Citizenship (SR 141.0, http://www.admin.ch/ch/f/rs/c141_0.html) actually makes no distinction between Swiss resident and Swiss abroad: Swiss citizenship is transmitted by birth. The only restriction is that Swiss born and living abroad, who also have another nationality, lose Swiss citizenship if their birth is not registered with the Swiss consular authorities by their 22nd birthday.

material to Swiss voters abroad. Recommendations for overcoming these problems, made in the ODIHR report of April 2008[9], include encouraging the introduction of e-voting. The recommendations have been followed up in the form of an implementation report[10].

This paper focuses on the development of e-voting with a focus on Swiss living abroad. The new channel is considered by the expatriates themselves to be the flagship measure to improve their ability to exercise their voting rights. After a short review of some facts and figures on Swiss abroad, their political rights and the implementation of these are explained, this paper will discuss the political decision to focus the development of e-voting initially on the needs of Swiss abroad and the different steps in implementing this decision, followed by a description of the expansion of the e-voting trials centered on those citizens living abroad since June 2008 (the date of the first Internet-voting trial for Swiss abroad which took place in the canton Neuchâtel) up to the last trials held in 12 cantons[11] during the federal elections of March 2012 as well as the trials in four cantons at the recent federal elections on October 23, 2011. It is observed that e-voting enjoys a high degree of acceptance among the population. A discussion of the future development of the project closes the paper.

2 Political Rights of Swiss Abroad and Their Exercise

By the end of 2011 there were some 700,000 Swiss abroad. According to the data collected during the last federal elections, about 125,000 of them have registered to exercise their political rights in a Swiss canton or commune[12]. The increase of more than 16% in the number of Swiss people living abroad within a decade is in part due to the increase in the number of people with dual nationality, in particular births abroad and naturalisation of family members. It is also a reflection of increased levels of migration, a trend, which can be observed worldwide. Almost 60% of Swiss abroad live in an EU country and about 25% in North America[13].

---

[9] OSCE/ODIHR Elections Assessment Mission, Report of 3 April 2008; see in particular chapter X, part C "Out of country voting", http://www.osce.org/odihr/elections/switzerland/31390.

[10] A detailed report on the implementation measures can be found under the Political Rights Section of the Federal Chancellery's website. The Federal Chancellery is the leading federal body responsible for the administration of votes and elections at federal level:
http://www.bk.admin.ch/themen/pore/nrw/index.html?lang=de -
See "*Implementation report OSCE/ODIHR*" on the right side of the page.

[11] The following cantons are involved in the e-voting project: Zurich (ZH), Berne (BE), Lucerne (LU), Fribourg (FR), Solothurn (SO), Basel-Stadt (BS), Schaffhausen (SH), St. Gallen (SG), Grisons (GR), Aargau (AG), Thurgau (TG), Neuchâtel (NE), and Geneva (GE).

[12] http://www.admin.ch/ch/f//pore/va/20110213/index.html (Click on "Details sur cet objet" to see the detailed figures.)

[13] To have more information visit the website of the Federal Department of Foreign Affairs:
http://www.eda.admin.ch/eda/fr/home/serv/livfor.html.

2.1 Political Rights of Swiss Abroad

The political rights of the Swiss abroad are set out in the Federal Constitution[14], the Federal Act on Political Rights for Swiss Abroad[15], and the Federal Ordinance on Political Rights for Swiss Abroad[16].

In the Swiss system of direct democracy[17], the Swiss abroad have the following political rights:

- Swiss abroad who are 18 and over are allowed to participate in all federal referendums and elections. Some cantons and communes also allow their expatriates to take part in votes and/or elections at cantonal level and some even at communal level.
- They have the right to elect and be elected.
- Swiss abroad are allowed to sign federal initiatives and referendums. Some cantons and communes also allow them to sign cantonal and communal initiatives and referendums as well.
- Swiss abroad have the same right as others to sign a petition.

2.2 The Exercise of Political Rights by Swiss Abroad

Swiss abroad can choose whether they want to exercise their political rights in their commune of origin or in (one of) their former domicile(s). In order to receive the voting material, they have to register with the Swiss consular representation in their country of residence.

In federal popular votes and referendums, an average of about 50% of these registered Swiss abroad cast their vote. In federal elections, the participation rate is lower; when it comes to choosing candidates for the national parliament, on average only around one-third of the registered Swiss abroad decide to participate.

Until 1992, those citizens living abroad had to come back to Switzerland to cast their vote in person. Since 1992, they have been allowed to send their vote by post. The material for postal voting is sent automatically to all registered Swiss abroad one week earlier than it is sent to residents in Switzerland. However, not all Swiss abroad can exercise their political rights, as the voting material may arrive too late in some countries due to difficulties with postal service[18]. In an attempt to find a solution to this problem,

---

[14] Federal Constitution of the Swiss Confederation as of April 18, 1999 (http://www.admin.ch/org/polit/00083/index.html?lang=en). There is a special article concerning Swiss broad (art. 40).

[15] Federal Act of December 17, 1976 on Political Rights (http://www.admin.ch/ch/e/rs/161_1/index.html).

[16] Federal Ordinance of May 24, 1978 on Political Rights (http://www.admin.ch/ch/d/sr/1/161.11.de.pdf [no English translation]).

[17] A form of democracy in which the participation of the People is comprised of both electing the highest state bodies and also determing whether and which issues should be submitted to the People for an official decision.

[18] Most delays occur in neighbor and European Union countries, typically: Italy, Spain, France .

the Federal Chancellery, the cantonal authorities responsible for political rights, and the Swiss post office founded a working group to investigate possible measures[19]. Some measures could already be applied for the 2011 national elections; others have yet to be implemented.

Due to these problems with postal voting, the Organisation of the Swiss Abroad (OSA)[20] began to demand the introduction of a remote, electronic voting channel a few years ago[21].

3 Focus on E-voting for Swiss Abroad

3.1 Context

In its second report on the "Vote électronique" project on May 31, 2006[22], the Federal Council[23] evaluated the five pilot trials conducted between 2004 and 2005 by the cantons of Zurich, Neuchâtel, and Geneva during federal referendums (for Swiss residents only). The report marked the end of the e-voting pilot phase and the beginning of a gradual and controlled introduction to e-voting.

The Federal Council was given the task of introducing e-voting on a gradual basis by the parliament. The Federal Council allotted this task to the Federal Chancellery, where the "Vote électronique" project was run by the Political Rights Section.

This strategy – along with the necessary legal amendments to enforce it – was approved by parliament on March 23, 2007[24]. While acknowledging the advantages of e-voting, the federal government opted for a gradual introduction of this additional voting method in Switzerland[25].

---

[19] For example, technical measures such as the format of the addresses or information on the envelopes.

[20] See also the organization's website http://aso.ch/en.

[21] A full, Internet-based voting procedure in which the voting material is also sent electronically to the Swiss abroad has yet to be realized and will not be implemented within the next few years due to various security-related difficulties.

[22] The report was published in the Federal Gazette 2006 5205; www.admin.ch/ch/f/ff/2006/5205.pdf .

[23] The Federal Council is the supreme governing and executive authority (Government) of the Swiss Confederation and is composed of seven members who are elected by the United Federal Assembly.

[24] On December 19, 2006 and March 19, 2007 the National Council and the Council of States respectively acknowledged the Federal Council report from May 31, 2006 on the e-voting pilot projects and amendments to federal legislation on political rights (the records of the two sessions can be found under the following URLs:
http://www.parlament.ch/ab/frameset/d/n/4715/236210/d_n_4715_236210_236330.htm (National Council) and http://www.parlament.ch/ab/frameset/d/s/4716/241444/d_s_4716_241444_241572.htm
(Council of States).

[25] Detailed information on the development of e-voting can be found, in English, in the three reports (2006, 2008 and 2010) that Switzerland (Federal Chancellery) transmitted to the Council of Europe in the context of the evaluation of implementation of the Recommendation 2004 11 on e-voting. Reports are available on demand.

The Federal Council authorised e-voting trials but limited them in order to minimise the risks. This approach reflected the technical and organisational challenges posed by the new voting method, as well as the risks it presented. Swiss abroad were identified as one of the groups with a major interest in e-voting.

The Swiss "Vote électronique" project consists of the following four phases:
- E-voting in federal referendums
- E-voting in federal elections
- E-collecting of signatures for federal initiatives and referendums
- E-collecting of signatures for federal election proposals.

A project team consisting of three members and a project manager is responsible for the operational and technical management of the project.
The cantons play the main role in the organisation of the project. In accordance with Switzerland's federalist structure, in which political rights are exercised differently in the different cantons, each canton is free to choose if and when it wishes to introduce e-voting.

3.2 Federal Legislation

The following amendments were introduced into federal legislation to enable the cantons to offer e-voting to their citizens abroad:

- **Article 8*a* of the Political Rights Act[26]:** This article stipulates that, in addition to the three pilot cantons, *interested cantons can begin controlled e-voting trials during federal votes*. Given that the results of electronic votes will have legal implications affecting the authorities, all trials are subject to prior authorisation by the Federal Council - the authority which validates the results of federal votes[27].

- **Article 5*b* of the Political Rights Act of Swiss abroad[28]:** This article stipulates that in order for Swiss abroad to be able to vote via Internet, *the electoral registers of Swiss abroad will be digitalised and either conducted in a centralised manner by the cantonal authorities or managed in a harmonised way by communes*. The cantons were given a year and a half , until the end of June 2009, to adapt their implementation provisions accordingly. In addition, work was also undertaken by the eCH-association[29]. The eCH-standard 0045[30] for voter registers, based on the international OASIS Election Markup Language Standard, was approved and has been already implemented by some cantons.

[26] See http://www.admin.ch/ch/f/rs/161_1/a8a.html.
[27] Art. 15, para 1, Political Rights Act.
[28] See http://www.admin.ch/ch/f/rs/161_5/a5b.html.
[29] This is the Swiss association for setting e-government standards. See www.ech.ch.
[30] See http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0045&documentVersion=1.00.

- **Article 27*c* of the Ordinance on Political Rights:** This article was modified in September 2009 to exclude Swiss abroad from the calculation of the quota limitation[31]. Given that they have the greatest interest in e-voting, and given the fact that they make up only a small proportion of the electorate, the federal government decided that Swiss abroad should be excluded from the quota limitation. This means that if a canton decides to introduce e-voting, it can offer it to almost all its Swiss abroad: namely those who live in EU and Wassenaar Arrangement States[32] as well as in certain small European countries[33]. Almost 90% of Swiss abroad live in these countries, which allow the exchange of encrypted data used in e-voting.

- **Article 27*k*^{bis} of the Ordinance on the Political Rights of Swiss Abroad:** This article was introduced in February 2010 to address certain aspects of the data exchange between cantons that cooperate to offer e-voting.

The amendments to the federal acts were adopted by parliament and were subject to optional referendum[34]; the amendments to the Federal Ordinance were approved by the Federal Council alone.

4 Introduction of E-voting for Swiss Abroad

4.1 Cooperation Between Cantons

In addition to amending federal and cantonal legislation in line with the goal of offering e-voting to expatriates, practical solutions had to be found to allow cantons without an e-voting system to start testing in a secure and cost-effective manner.

At the conclusion of the pilot phase, the Confederation, which contributed financially to the realisation of the three different e-voting systems in Zurich, Neuchâtel, and Geneva, decided to end any financial participation in future e-voting trials[35]. In accordance with previous agreements, the three pioneering cantons agreed to publicly release their know-how and the final results obtained to any interested cantons at no cost. In practice, this gave rise to some innovative types of inter-cantonal cooperation. The three pilot cantons,

---

[31] During the pilot phase, the Federal Council limited the possibility of voting electronically to 2% of the Swiss electorate. During the 2007-2011 legislative period, the Federal Council made sure that the level did not exceed 10% of voters at federal level, even as more authorizations were granted. In the case of mandatory referendums, where the majority of cantons also play a decisive role, the Federal Council made sure that these trials did not involve more than 20% of voters in each canton.

[32] Wassenaar Arrangement of December 19, 1995/May 12, 1996 on export controls for conventional arms and dual-use goods and technologies, www.wassenaar.org. The Arrangement regulates the export/import of cryptography, a dual-use technology.

[33] Andorra, Liechtenstein, Monaco, San-Marino, Vatican State, and the northern part of Cyprus.

[34] The optional referendum is a popular vote that is held if requested by 50,000 voters or eight cantons on a new amended federal act, decree, or certain international treaties. The referendum bill is approved if a majority of those voting vote in favor of it.

[35] A detailed overview of the costs of e-voting will be presented in the third report of the Federal Council in 2013.

which each own and operate an e-voting system, and which have relatively long experience with e-voting, offered the use of their systems to other cantons. Therefore, the solutions developed in the pilot cantons can be employed by other cantons.

Two forms of cooperation have emerged:

- The *hosting solution* offered by the canton Geneva (see 4.2)
- The *consortium solution,* which operates a copy of the canton Zurich system (see 4.3).

Neuchâtel, which is the only canton so far to have developed a comprehensive online portal of cantonal government services (GuichetUnique.ch), of which e-voting is a feature, has yet to develop a scheme offering e-voting to other cantons.

4.2 Hosting Solution

In the hosting solution, the hosted canton transfers its electoral roll to the hosting canton. The hosting canton uploads the roll to its e-voting system and starts operating the system. When voting has ended, the hosting canton opens the ballot box, obtains the results, and transmits them to the hosted canton. To date, Geneva has signed hosting contracts with Bern, Lucerne, and Basel-Stadt[36]. The Federal Chancellery is also part of the hosting agreements. To make sure the Geneva e-voting system satisfies the needs of all hosted cantons (including the needs of Geneva itself), a user group[37] has been created.

4.3 Consortium Solution

The consortium solution was formed in autumn 2009. Seven cantons[38] agreed to cooperate to use a copy of the Zurich e-voting system, operated by a private company. The consortium solution is similar to the hosting one, with the major difference being that the system is not operated by a canton, as in the Geneva case, but by a private company. The Federal Chancellery is part of the consortium's agreements as well.

Both hosting and consortium solutions offer several advantages, not least of all lower costs for the joining cantons (compared to the cost of developing/buying yet another system). It also gives those cantons an opportunity to trial e-voting in a secure and cost-effective manner and discuss its future extension. Plus it allows participating cantons to resolve problems faced by voters abroad.

---

[36] The first hosting contract was signed in Berne in June 2009: http://www.bk.admin.ch/aktuell/media/03238/index.html?lang=fr&msg-id=27425.

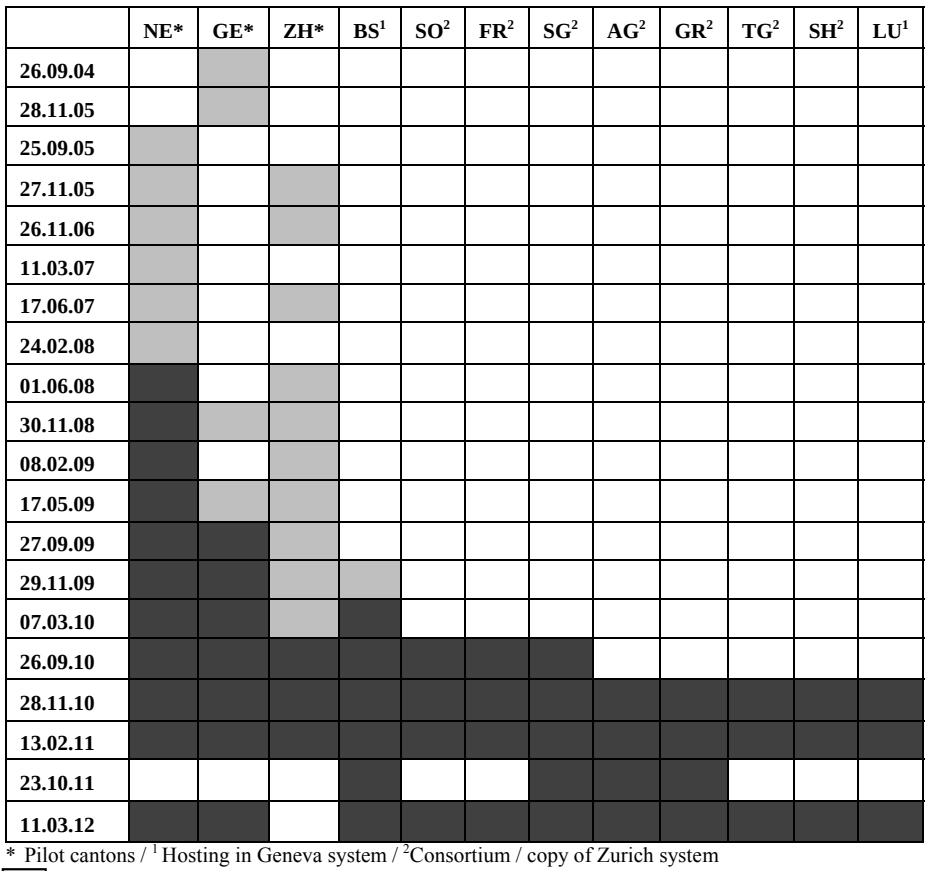
[37] The user group has the competence to decide upon the development/modification requests coming from the partners; deal with the organisation of votes/election, the technical specifications, fix priorities, and handle costs; decide the functional modifications of the system which can impact the hosted cantons; take stock of the last trial as it meets Monday, 8 days after every voting Sunday.

[38] Fribourg, Solothurn, Schaffhausen, St.Gallen, Graubünden, Aargau, and Thurgau.

5 Implementation of E-voting

5.1 Implementation for Referendums and Elections

Since 2004, 75 trials have been conducted in federal popular votes and four in federal elections, making a total of 79 trials. The systems were employed at numerous cantonal votes and communal votes as well.



* Pilot cantons / [1] Hosting in Geneva system / [2]Consortium / copy of Zurich system

Trials without Swiss voters abroad

Trials with Swiss voters abroad

Fig. 1: E-voting trials (at federal level)

For each ballot, as many as 170,000 voters were able to vote electronically. This did not exceed the limit of 10% of the electorate set by the Ordinance on Political Rights.
It is not possible to discern from the statistics whether or not the introduction of e-voting had an influence on the number of Swiss abroad who voted. Only very few of the cantons identify votes cast by Swiss abroad separately. Nevertheless it is worthy mentioning that there has been an increase in the number of Swiss voters registered abroad since e-voting was introduced. Research has not yet been conducted into whether these two facts are connected.

5.2 Focus National Elections 2011

On October 23, 2011, e-voting was used for the first time in federal elections. Approximately 22,000 Swiss voters abroad, registered in the cantons of Basel-Stadt, St.Gallen, Grisons, and Aargau, were permitted to use this system. This was about 0.4% of a total of approximately 5,090,000 voters. About 53% of Swiss voters abroad, who were registered in the cantons entitled to take part in the trial, made use of this new voting method. The e-voting trials ran smoothly. The technical and logistical challenges were successfully mastered by the cantons involved. This first-ever use of e-voting in federal elections marked the beginning of the second phase in its implementation.

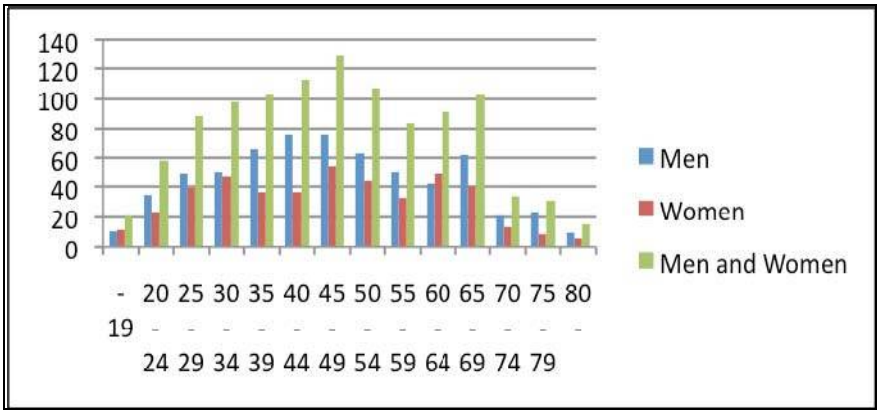


Fig. 2: Voter participation among Swiss abroad registered in canton Grisons using e-voting, by age group (Source: Grisons Cantonal Chancellery)

An analysis of voter participation among Swiss expatriates registered in the canton Grisons shows that e-voting is used most frequently by men in all age groups. Most of the people who use e-voting are aged 45-49. The distribution is normal.
The 2011 elections to the National Council were observed by the OSCE/ODHIR. The team of experts was particularly interested in the e-voting systems, as this technology is relatively new and to date, pilot studies only been conducted in a few member countries. The report was issued on January 30, 2012[39].

[39] http://www.osce.org/odihr/elections/Switzerland/81974.

6 Acceptance and Use of E-voting

The results of a survey conducted in 2011 by the Federal Office of Communications showed that there is considerable support for an electronic voting system and the public perceives a need for trials to be continued[40]. Another public survey conducted in 2011 by the Federal IT Steering Unit confirms that the general public would like to see e-voting given priority in e-government programs[41]. Surveys carried out in the cantons also suggest that the project is widely accepted. In 2011, the canton Geneva gave the whole electorate an opportunity to vote online in two cantonal votes, of which just under 20% of the electorate made use of the option. This ballot showed that e-voting has clearly become accepted as a third valid voting option. On this occasion, online voters were surveyed. 80% claimed to be very satisfied with the voting process in terms of user-friendliness and time taken to vote. Just fewer than 40% were using e-voting for the first time. Two thirds said they would use e-voting again at the next ballot. Very few people contacted the helpdesk, which suggests that the system was easy to use.

Nevertheless, some cantons are experiencing opposition to e-voting. As an example, a motion entitled "E-voting Is Dangerous for Democracy – Let's Stop the Expense" was submitted in the canton of Vaud, signed by representatives from almost every political party represented in the cantonal parliament[42]. The motion calls for a total ban on e-voting. The main arguments relate to the transparency, security, and secrecy of e-voting. Further arguments include the privatisation of processes meant to be public and the trivialisation of the act of voting. At the federal level, an interpellation entitled 'Electronic Voting: A Danger to Democracy' has been submitted to the Council of States[43]. It questions the security and organisational aspects of Internet voting.

The Confederation and its partners take doubts and fears expressed by critics seriously. Emphasis is placed on enhancing security and transparency so as to foster trust in the new voting channel. These objectives form the focus of ongoing and future work on e-voting (federal group on e-voting and its taskforces, see 7.2).

[40] For all results see: http://www.uvek.admin.ch/themen/kommunikation/00690/01347/index.html?lang=de.
[41] http://www.egovernment.ch/studienportfolio/upload/pdf/E-Government_Bevoelkerung_Bericht_def.pdf
[42] Vaud Cantonal Parliament (accessed 17.01.2012): http://www.vd.ch/fr/autorites/grand-conseil/seance-du-8-fevrier-2011/motion-jean-christophe-schwaab-le-vote-electronique-est-dangereux-pour-la-democratie-arretons-les-frais/.
[43] Smaller chamber of the Federal Parliament that is composed of 46 representatives of the cantons.

7 Outlook

7.1 "Vote électronique" Roadmap

Drawn up in spring 2011, the "Strategic Paper on Vote Électronique" (roadmap)[44] provides an overview of the rollout strategy for the coming years. It lays down common objectives and milestones so as to ensure optimal coordination between the Confederation and the cantons and defines measures to drive the project forward. The strategy, which was discussed by the Conference of Government Chancellors at its spring meeting in 2011, provided for the establishment of a nine-member steering committee responsible for dealing with all strategic and political issues. The creation and first constituent meeting of the steering committee, which consists of representatives from the Confederation and the cantons, took place in Bern in August 2011 under the auspices of the Federal Chancellor. This new coordinating body is charged with supporting the ongoing implementation of the project and studying future strategic proposals. Following its formation, the steering committee intends to meet at least twice a year and its purpose is to assess the progress of the project and monitor the implementation of the roadmap objectives.

7.2 Security Standards Taskforce

Due to current legislative limitations, only the Swiss abroad and a limited proportion of citizens resident in Switzerland may use e-voting. Since the impact of certain risks increases with the number of voters using e-voting, the roadmap foresees the granting of e-voting access to more users only after crucial security questions have been revisited. The roadmap therefore serves as a basis for the newly founded security standards taskforce. The group, comprised of representatives from the Confederation, cantons, academia, and various consulting firms, aims to establish a set of minimal security criteria that e-voting systems and their administration need to comply with before the community of users can be expanded.

An absolute key requirement of e-voting systems is that they need to generate results as the consolidated collection of legitimate votes (which have not been tampered with). As ballot secrecy has to be maintained at all times, fraud attempts are not as easily detectable as with other Internet applications, such as e-banking. Nevertheless, the technical literature on e-voting cryptography suggests a multitude of privacy-preserving solutions, such as verifiable protocols that allow voters to verify that their vote has reached the voting servers as intended, that it has been recorded as cast, and tallied as recorded. The taskforce seeks to increase security requirements and relate its reflections to the existing literature. With this aim, Bern University of Applied Sciences' (BFH) e-voting research group of has been given the task of producing a concept outlining how

[44] See: http://www.bk.admin.ch/themen/pore/evoting/06552/index.html?lang=de.

a verifiable system could be implemented in practice[45]. The Norwegian experience, with their trial using a verifiable system in September 2011, serves as a fine source of inspiration in terms of usability and the implementation of a verifiable protocol in practice.

The security standards taskforce has assumed the user's platform to be the most vulnerable system component. In Norway, the problem has been mitigated by introducing return codes that enable voters to verify whether their vote has been tampered with before arriving at the servers. While Switzerland is looking at Norway's solution with great interest, the Confederation has also given a grant to the Federal Institute of Technology in Zurich (ETH) to elaborate on this sensitive subject and propose appropriate solutions. An ETH-researcher is also a member of the security standards taskforce, continually sharing newly discovered insights. Regardless of which final technical requirements will be proposed by the security standards taskforce in summer 2012, there will also be organisational requirements to consider, such as requirements on external audits.

7.3 Expansion of E-voting

Some cantons are planning to expand their e-voting projects. The next steps will include offering e-voting to Swiss residents and implementing e-elections. Other cantons have expressed an interest in introducing e-voting for their own expatriates. The Federal Chancellery, as the coordinating body, supports the cantons in implementing their chosen solution. It has set itself the goal of permitting the majority of eligible Swiss voters abroad to cast their ballots electronically in federal votes and referendums by 2012 and in elections by 2015. As governments gain e-voting experience through their expatriates, e-voting will gradually be made available to Swiss residents as well.

While there are some critics, a strong political will to develop Swiss e-voting can be observed among the many stakeholder groups. In September 2011, a parliamentary intervention asked for the introduction of a federal obligation for cantons to introduce e-voting for their Swiss abroad by the next elections in 2015[46]. Even though the Federal Council is in favour of introducing e-voting, it rejected this proposal, as the cantons, which are responsible for organising national polls, should be free to decide if and when they wish to begin this complex project. This also fits in with the ongoing cooperative approach. The Organisation of the Swiss Abroad is currently collecting signatures for a petition demanding the introduction of e-voting for all Swiss citizens.

[45] http://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de.

[46] Motion Fässler (Flächendeckendes E-Voting für Auslandschweizerinnen und -schweizer bis 2015), see http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113879.

The Federal Chancellery has been evaluating the trials conducted since 2006. This evaluation will lead to a third report on "Vote Électronique", which is due to be presented to the Federal Council by mid-2013. The report will also make recommendations on how to proceed with the project. At the same time, the current legal basis for e-voting will be reviewed and proposals for modification will be made to the Federal Council, which is in charge of amending the Federal Ordinance on Political Rights.

8 Conclusions

Swiss voters abroad are the target group prioritised in the introductory phase of the "Vote Électronique". First, the possibility of voting online satisfies a particular need of this target group. Secondly, Swiss voters abroad form a clearly defined group which can be easily monitored. This is particularly important in the pilot phase.
Since 2000, binding trials with e-voting have been carried out in Switzerland. So far 13 cantons have become involved in the project. Finding solutions to extend e-voting to Swiss abroad from cantons that have no e-voting system has fostered a new cooperation between cantons as well as with the Federal Chancellery. Extending e-voting as part of a gradual process has proven its worth.

Thanks to the "Vote Électronique" roadmap, the players involved in the project have had the certainty they need to proceed with planning and investment. By 2012, the majority of Swiss voters abroad should be able to participate in popular votes and referendums online. In 2015, thanks to "Vote Électronique", the large majority of Swiss voters abroad should be able to cast their votes in the federal elections.

The success of the Swiss model of the introduction of e-voting can be explained by the following elements: joint strategic planning, positive inter-cantonal cooperation with hosting solutions, and a gradual expansion with an intense focus on security. The third report of the Federal Council is due in 2013 and will evaluate the trials carried out so far, establishing the conclusions of the security standards taskforce as well as the next steps to be taken.

Among Swiss voters abroad, e-voting has established itself as a safe, practical means of voting alongside postal voting. At the same time, the political parties are showing greater interest in mobilizing this target group. Such interest in the votes of expatriates almost automatically means that measures that made it easier to cast votes, such as the introduction of e-voting for federal elections, have been embraced by almost all political parties.

Bibliography

[CE11] Chancellerie de l'Etat de Génève, Second scrutin en ligne ouvert à tout le canton: Grande satisfaction des utilisateurs, Genève, 2011
Available on: http://www.ge.ch/chancellerie/communiques/2011/20111127.asp

[EG11] E-government Schweiz, Studie Bevölkerung und E-Government, Berne, 2011
Available on: http://www.egovernment.ch/studienportfolio/upload/pdf/E-Government_Bevoelkerung_Bericht_def.pdf

[FO11] Federal Office of Communications, Thesen zur Entwicklung der Informationsgesellschaft in der Schweiz: Ergebnisse der Online-Umfrage, Berne, 2011
Available on: http://www.uvek.admin.ch/themen/kommunikation/00690/01347/index.html?lang=de

[OS08] Organisation for Security and Cooperation in Europe, Elections Mission Report of 3 April 2008, Vienna, 2008,
Available on: http://www.osce.org/odihr/elections/switzerland/31390

[SF04] Swiss Federal Chancellery, First report on "Vote électronique", Berne, 2011. Available on: http://www.bk.admin.ch/themen/pore/evoting/06552/index.html?lang=de

[SF06] Swiss Federal Chancellery, Second report on "Vote électronique", Berne, 2006
Available on: http://www.bk.admin.ch/themen/pore/evoting/06552/index.html?lang=de

[SF11] Swiss Federal Chancellery, Implementation report OSCE/ODHIR, Berne, 2011, http://www.bk.admin.ch/themen/pore/nrw/index.html?lang=de

[SFC11] Swiss Federal Chancellery, Roadmap "Vote électronique", Berne, 2011
Available on: http://www.bk.admin.ch/themen/pore/evoting/06552/index.html?lang=de

E-voting at Expatriates' MPs Elections in France

Tiphaine Pinault, Pascal Courtade

Ministry of the Interior,
Bureau des élections et des études politiques,
Place Beauvau, 75008 Paris, France,
{tiphaine.pinault | pascal.courtade}@interieur.gouv.fr

The electoral law in France has been adapted to introduce e-voting. This voting method is however restricted to the eleven constituencies of French citizens living abroad in order to cope with the specificities of this electorate, notably its remoteness from polling stations. The legal framework as well as the technical solution was built in order to preserve the general principles applying to a political vote such as secrecy and sincerity.

Since the 2008 constitutional review, French expatriates have their own MPs at the lower Chamber of the Parliament[1], who will be elected for the first time in May and June 2012. Due to the specificities of the expatriates population, especially the remoteness they sometime experience from their polling station, the Government and the Parliament opened several voting methods, among them electronic voting. The general election is to take place in France on Sunday 10th June and Sunday 17th June 2012, and the e-voting will take place from Wednesday 23rd May to Tuesday 29th May for the first round and then from Wednesday 6th June to Tuesday 12th June for the second round.

The implementation of e-voting in the French electoral law required the drawing up of both a regulatory framework and a technical solution, both compliant with the general principles applying to political elections. The article will therefore present steps taken by the legislation in order to ensure the compliance of various principles, as well as a description of the electoral operation and their compliance with security requirements set by independent French national authorities.

As this article has been submitted (February 2012), the parliamentary election has not taken place yet. So far, the e-voting solution built in France has only been tested during a mock election that took place in January 2012.

[1] For further information, see: http://www.diplomatie.gouv.fr/fr/les-francais-a-l-etranger/elections-2012-votez-a-l-etranger/les-elections-en-2012-a-l-etranger/

1 E-voting for Expatriates' MPs to Be Elected in Eleven "New" Constituencies

The French Constitution was reviewed on the 23rd of July 2008 in order to enable French expatriates to elect their own MPs. Eleven constituencies were created. Prior to this constitutional review, expatriates were granted the right to elect representatives at the Assembly of French expatriates. This assembly does not have a legislative power, but is meant to represent expatriates in relations with government departments. Since 1982, its members are elected by expatriates, and in 2003, e-voting was introduced for these elections.

Despite the huge French consular network, voting for the 1.1 million expatriates registered on a consular election board can sometimes be a complicated process, due to the geographical distance between the voter and his designated polling station[2]. Hence, the participation rate of voters living abroad is lower than the medium rate in France (see figures below).

Presidential election – Participation rate			
1st round	1995	2002	2007
Expatriates	50,87%	37,27%	40,30%
National average	78,38%	71,60%	83,77%
2nd round	1995	2002	2007
Expatriates	53,01%	44,22%	42,13%
National average	79,65%	79,71%	83,97%

Table 1: Participation in Presenditial elections 1995-2007

Such difficulties and the wish to boost participation encouraged the Parliament to grant expatriates four channels of vote casting at the parliamentary election: going to the polls, proxy-vote, postal mail or Internet.

This latter possibility is introduced for the first time into the French electoral law. Indeed, e-voting has not yet been experienced at a political election. Some limited experiments were done in the field of electronic democracy in the recent past. For instance, e-voting was implemented for trade-union elections at the Department of Education and for the election of the 155 counsellors of the Assembly for French expatriates[3] in 2006 and 2009. The introduction of e-voting did not have a noticeable impact on the participation rate[4] for this election. However, the French Government hopes that this new means as well as the creation of a specific representation for expatriates will increase the participation rate.

[2] Expatriates can vote at the embassy or in the consulate of the consular constituency they are attached to.
[3] The Assembly for French expatriates is not a political body.
[4] Participation rate: 24,08% (1997), 18,97% (2000), 21,82% (2003), 14,25 % (2006) and 20,44% (2009).

In 2009, when the law implementing the constitutional review was passed[5], the political choice was to limit e-voting (as well as postal voting) to the election of the 11 expatriates' MPs and not to extend it to the other elections expatriates are entitled to vote for, such as the presidential election or referendums. This choice can be explained by the different nature of the presidential election and of the parliamentary election: the first is based on a single national constituency whereas the second is based on 577 constituencies. Therefore it would be problematic, with regards to the principle of equality that expatriate voters dispose of more voting options than voters living in France or in overseas territories.

Electronic democracy is a matter of controversy in France, where a part of the population proved suspicious about electronic voting machines introduced for political elections since 2000. Quite a number of citizens went to court to call for elections to be canceled. Therefore, the Government decided to freeze the extension of voting machines in the municipalities that did not own them in 2008. For these reasons, there is no doubt that the electronic voting taking place in May and June will be highly scrutinized by opponents of electronic democracy. However, the system put in place has been designed to enable the constitutional principles and numerous control mechanisms have been implemented at different stages, notably by independent auditors.

2 A Long Process to Design the Regulatory Framework

The implementation of e-voting for expatriates' MPs required a strong cooperation between the Ministry of the Interior, in charge of the organisation of political elections, and the Ministry of Foreign Affairs responsible for the consular network involved in the electoral process. Both departments participated in the design of the legal framework, as well as the design of the technical solution.

Numerous independent authorities were also part of the design of the solution, among them the ANSSI (independent national agency in charge of ensuring the security of state information systems) and the CNIL (French independent authority in charge of personal data protection) and various auditors.

The 2008 constitutional review was completed by two laws, one in July 2009 (an ordinance) and one in April 2011[6] and by a decree signed on the 15th of July 2011[7]. The two laws passed by the Parliament opened the possibility of e-voting. The legislative part of the election law does not regulate the electoral operations in details.

However, the law foresees that a decree will be enacted, that ensures that electronic voting tools "respect vote secrecy and the sincerity of the election". It has to be noted that the legislative process in France imposes that before a bill is submitted to the

[5] Ordonnance n°2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France

[6] Loi organique n°2011-410 du 14 avril 2011 relative à l'élection des députés et des sénateurs.

[7] Décret n°2011-843 du 15 juillet 2011 relatif à l'élection de députés par les Français établis hors de France.

Parliament, it has to be examined by the Administrative Supreme Court. According to this court, e-voting is an acceptance between the constitutional principles of sincerity and secret of the vote and of access to the vote. No appeal was made against the text.

The decree (eleven articles) details the electoral operations, the main security requirements and the role of the polling station. According to the French legislative process, the 2011 decree, and each text on e-voting had to be submitted to the French independent authority in charge of personal data protection, before its publishing, in order to guarantee that e-voting respects provision of the 1978 law on data protection.

The responsibility of the data processing is given to the ministry of the interior and the ministry of foreign affairs. The decree foresees that before its implementation, the e-voting software has to be audited by an independent expert.

Both ministries are also in charge of the certification of the system. The certification is foreseen by a 2010 decree[8], which imposes that each State authority creating an information system has to certify to its users that it respects the security objectives set in the decree. The certification of the French system took place in March 2012: the secretary general of the MFA and of the MOI acknowledged that nothing more could be done to tackle residual risks, which have been reduced to the minimum. The certification was conducted under the scrutiny of the ANSSI, the independent national agency in charge of ensuring the security of state information systems. Before the certification, the ANSSI audited the architecture of the system, its code, and the hosting infrastructures of the system.

The decree specifies the list of members of the e-voting polling station, as well as the nature of their mission: it is composed by a member of the French Supreme Administrative Court, a member of the Ministry of Foreign Affairs, a member of the Ministry of the Interior, a member of the national agency for security of information systems, and three members of the Assembly of French abroad. Therefore, its composition is balanced between elected members, civil servants and technical experts of information systems. Only members of the e-voting polling station own fragments of the decryption keys. Additionally, there have to be at least 4 (the quorum) members out of 7 to generate the entire key.

The presence of members of the e-voting polling station is mandatory for the closing of the electronic ballot box and for its opening after the end of the voting process. Its mission is to ensure that electoral operations are managed properly. Publicity of the voting operations can only be limited by members of the e-voting polling stations in order to preserve the security of the process. Each issue that might occur during the vote has to be documented in the voting protocol. The communication of theses minutes obey to the general rule set in the electoral code (article R.70), meaning that each voter can ask for access to these documents to contest the electoral operations.

[8] Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

To protect the secret of the vote and fulfil anonymity requirements set by the law on privacy, the decree foresees that the voting ID should have not any link to the identity of the voter. This separation is set by the CNIL for each generated vote or file including personal data. Moreover, the voting ID is generated on an unpredictable basis. Finally, the ID and the password are sent by two separate means of communication.

The regulatory framework had to ensure the balance between the electoral principles, like election sincerity and vote secrecy (both are constitutional principles), protection of personal data and the objective of the reform to lessen difficulties faced by expatriates when going to the polls.

It was decided not to introduce a "right to regret" (vote multiple times) as some countries have. Hence, once the e-vote is cast, the voter is registered on the list and will not be able to vote in the polling station if he tries to. On the Election Day, authorities will have the list of voters who already cast their ballot.

3 The Technical Solution Had to Comply with the Constitutional Principles Ruling the Election

The focus of the authorities has been on the development of a user-friendly technical solution enabling e-voters to vote in one single session. The consortium in charge of the development of the e-voting system was chosen according to French procurement rules. The development of the voting system started a year before the election. All along the process, the Government delegated the project controlling to the French independent authority in charge of personal data protection (the Commission nationale de l'informatique et des libertés[9]).

The e-voting system had to fulfil important security requirements entitled by the 1978 law on protection of personal data and the specifications mentioned in the decree. Thus, the decree details the basic requirements written in the law and mentions that data created for the electronic vote has to guarantee the separation, in distinct files, of the data related to the identity of the voter and of the data related to the ballot.

Several controls were foreseen by the decree to ensure both the preservation of the vote secrecy and the sincerity of the election. Two audits are being run on the system built by Atos-Scytl: one by the national agency (ANSSI) in charge of ensuring the security of information systems, and a second one run by an independent audit agency. Moreover, a risk analysis has been conducted, according to the EBIOS method to ensure the utmost level of security.

To preserve the secrecy of the vote, the system relies on a strong identification of the voter. Anyone who is not identified by the system is not able to vote online. There is no pre-registration system for the use of e-voting at the general election day. Voters

[9] http://www.cnil.fr/english/the-cnil/

registered on a consular election board are able to decide to use e-voting: each will be sent an ID by postal mail 15 days prior to the election. It will be valid for both rounds. It will be sent a second time by short message ten days before the first round. A password will be sent by email 5 days before each round, it will be different for both rounds. To secure the voter's computer, the connection to the e-voting website generates a secure electronic voting booth on the voter's machine. After he/she casts his/her vote, the voter is sent a receipt.

To ensure the sincerity of the election, the e-voting system and the ballot box have to be proofed against security breaches to assure that no one is able to enter the system while the poll is still opened and that fake ballots cannot be added to the voters' ballots. The system is operated by a two-key system. A public key ensures the encryption of the date while a private key ensures its decoding. The two keys are generated at the beginning of the poll, when the electronic polling station is opened. During the voting process, only the public key exists, the private key is being destroyed. Ballots and vote receipts are stored in a ceiled envelop. After the election is closed, both keys are necessary to start the counting of the ballots. Each operation is registered, so that members of the polling station should be able to notice any breach in the system and that any operation is detected that is not due to occur.

The whole voting process is supervised by an electronic board (EPS) composed of eight members. It is chaired by a magistrate and other members are either state officials, representative of the national agency for security of information systems, or members of the Assembly for French expatriates. Similarly to the right granted during traditional voting operations, each candidate can designate a delegate tasked with the observation of the voting operations.

The role of the EPS is to ensure the correctness of voting operations. At the beginning of the vote, the EPS ensures that the digital ballot box is empty and that the list on which each voter signs after casting the ballot is blank. At the end of the vote, members of the EPS sign the minutes of the voting process. In order to ensure the sincerity of the vote, members of the polling station have investigatory power and can decide to stop voting operations either temporarily or permanently.

4 A Mock Parliamentary Election Enabled Authorities to Test the Security and the Efficiency of the System

In order to test the e-voting system, both Departments decided to run an extensive test in January. 15.000 voters, registered on consular electoral boards volunteered to participate in this large-scale test. Participation was 30% for the first round and reached 33% for the second round. During the test, the ANSSI simulated various attacks to test the security of the system.

The outcome was considered positive and the e-voting system itself qualified. However various practical difficulties occurred that needed to be solved before the election day in May and June.

Indeed, the main difficulties concerned the accessibility of the voting site (compatibility of the voter's computer) and identification difficulties. The test raised the awareness of the Ministry of Foreign affairs to take actions to solve the issues revealed by the full-size test. The MFA created a testing system, which can be used by the voter, prior to the election day, in order to ensure that the computer is compliant with the voting site. Moreover, the assistance unit will be increased on election day to provide a quick support to each voter experiencing difficulties.

In order to cope with any difficulties preventing someone from voting on the day of the genuine election, each voting channel will be available at different times: first the e-voting, then postal voting, and finally voting at the polling station and proxy vote. This scheduled voting process aims at securing the ability to vote in any case for each voter.

First lessons learnt from the test proved that introducing a new voting method requires a strong communication effort so that voters are prepared to use e-voting and are able and confident to vote electronically.

A long term communication campaign was built by the Ministry of Foreign affairs, first to collect updated contact information from French expatriates to inform them of the option to vote electronically and for receiving their passwords and ID.

Very practical difficulties occurred during the test, such as delays due to dysfunction of postal services in several countries, or incompatibility of the voting software with some computer operating systems.

* * *

In conclusion, the regulatory framework and the technical solution developed to enable French expatriates to elect their own MPs electronically were meant to measure up to the importance of the event. Political elections are regulated by intangible constitutional principles that ought to be respected. Audits and tests proved essential to tackle security weaknesses and organisational difficulties. The full-size test proved successful but also indicated there was room for improvements in the organization of e-voting. The test revealed practical difficulties, such as accessibility to the voting site or reception of identification and certification material in time for the vote. These issues have been addressed for the general Election in June.

Session 7

Practical Experience with E-voting

The New Belgian E-voting System

Carlos Vegas González

PhD Reseacher on Constitutional Law
EVOL2 / eVoting Legal Lab (DER2010-16741), Spain
carlos.vegas@europe.com

Abstract: In use since 1994, the Belgian e-voting system has reached the end of its useful life. A new prototype (an improved paper-based voting system), developed by a consortium led by Smartmatic, will be used for the first time in October 2012. This paper takes a look at the workings of the new system and carries out a brief analysis of its compatibility with the main international election standards.

1 Introduction

A new e-voting prototype will be used for the first time in Belgium's upcoming regional elections in October 2012 and is meant to replace the old voting machines, which have been in use since 1994.

The system is based on a proposal developed, at the request of the government, by a consortium of Belgian universities and presented in a comparative study on e-voting. Although the study was partially granted the green light in a 2008 report from the Council of Europe and an October 2011 test of the new system took place with very few problems, some issues still remain open: among them are the concerns of some political parties and civic associations regarding the transparency of the system. It should also be pointed out that, although the new system will be implemented in the Flanders and around Brussels, the Walloon Region seems to be working on developing its own system.

After an outline of the history of e-voting in Belgium (§ 2), this paper will examine the 2007 BeVoting study and the 2008 Council of Europe Report (§ 3). It will then focus on the functionality of the new system and the tests carried out in 2011 (§ 4) and will finally take a look at some issues that may still remain open to discussion, especially in regards to international election standards for e-voting (§ 5).

2 Historical background

Belgium was one of the first countries in the world to use e-voting technology. Following an initiative from the Minister of the Interior in 1989, the Federal Parliament approved a law[1] in July 1991 in order to start testing two different e-voting systems[2] in two electoral cantons (Waarschot in Flanders and Verlaine in Wallonia) for the parliamentary and provincial elections of November 1991.

After that first experience, a system based on a magnetic card[3] was chosen to continue with e-voting, and a law[4] was passed in 1994 establishing the general framework for e-voting in the country. E-voting was expanded throughout Belgium in two waves: in 1994 1.4 million voters participated (20% of the voters) and in 1999 over 3.2 million[5] voters (44% of the voters) cast an e-vote.

Although the expansion of e-voting to the rest of the country had been officially planned, no further extension has taken place since 1999, and the same municipalities that piloted the program continue to use it today[6].

E-voting created some controversy in Belgium for several years. According to the OSCE Election Assessment Mission for the 2007 Federal Elections see [Os07, p. 10]: "*While the overall technical performance of the e-voting procedures would not appear to be fundamentally questioned, some political party officials, in particular of the French-speaking side, and civic group activists, have expressed concerns about e-voting. The focus of their criticism largely stems from concern with regard to the lack of effective public oversight of e-voting*". We can indeed find some contentious incidents[7],

---

1 Loi du 19 juillet 1991 organisant le vote au moyen de systèmes automatisés dans les cantons électoraux de Verlaine et de Waarschot, published on the Moniteur belge on 3 Septembre 1991.

2 One of the systems tested during those elections was based on a touch panel similar to those used in the Netherlands. The other system (used last in the 2010 federal elections) was based on a magnetic card and a voting machine with a light pen.

3 Currently, there are two e-voting systems in Belgium: "Digivote" (STERIA) which covers approximately 85% of the market and "Jites" (STESUD) which covers approximately 15% of the market. It is up to the municipalities (communes) that opted for e-voting to choose which system they will use, but since the two systems are incompatible, all municipalities within one single canton must agree on the same system. With the current system, the voting process starts with the voters indentifying themselves to the Polling Station Chair and receiving a magnetic ballot card. In the polling booths, voters insert the card into a computer and the candidate lists appear on the screen. When choosing from the candidate list in the computer, the vote is recorded on the magnetic card. The voter then shows the card to the Polling Station Chair for verification that there are no marks and inserts it into an electronic ballot box. Votes are read from the card by the electronic ballot box and saved to the RAM and on ballot box's hard drive.

4 Loi du 11 avril 1994 organisant le vote automatisé (http://www.bruxelleselections2006.irisnet.be/download/06.pdf), modified by loi du 12 août 2000 (Moniteur belge du 25 août 2000) is the main law regulating e-voting in Belgium.

5 In Wallonia 39 municipalites out of 262 (22% of the voters), in Brussels-Capital all the municipalies (100% of the voters) and in Flanders 143 municipalities out of 308 (50% of the voters) are utilizing some form of e-voting.

6 2000 local elections, 2003 federal elections, 2004 regional and European elections, 2006 local elections, 2007 federal elections, 2009 regional and European elections and 2010 anticipated federal elections.

7 For example an e-voting problem reported in the local elections of 2003 in Schaerbeek in which one candidate got 4096 extra votes.

opposition from some civil society groups[8], and concerns expressed by some members of the Parliament and Senate[9] toward e-voting. In regards to these parliamentary controversies, the OSCE had already pointed out during an OSCE expert-visit on new voting technologies [see Os06 pag 4] that apprehension "*seems to be the main reason why the use of e-voting in Belgium has not been extended beyond the current 44% of the electorate using it since 1999. Some of the actors met complained that little or no debate took place when the experiment started, and the e-voting system has never been the object of a national evaluation/discussion.*" Furthermore, the OSCE pointed out that "*the procedure, which did not provide for a voter verifiable paper trail, is being criticized in some fora for lack of transparency.*" Critics say that the system suffers from a perceived "*limitation of possibilities for democratic control, with a particular emphasis on the absence of a voter verifiable auditable paper trail*."

Due to the issues mentioned above, new security measures and controls were added at different stages:

1. The Ministry of Interior published the source code of the voting software on its website (done on election day after the closing of the polling stations).
2. The creation of the College of Experts[10], an "independent" expert committee,to monitor the use and proper working of automated voting systems.
3. The certification of the hard- and software by an independent external company. The company needs to have been approved (*accréditation*) by the Council of Ministers as able to certify e-voting systems in accordance with the law and is chosen following an assessment of its application, This procedure began in 2003 following a recommendation from the College of Experts.
4. The introduction of an automated optical-reader counting system called "Favor" for the elections in 1999, 2000, and 2003, in which voters cast their votes using traditional ballot papers, which were then scanned by an optical reader.
5. The introduction of a "ticketing" system for the 2003 elections in the two locations that originally started e-voting. This new system added a paper trail (VVPAT) to the previous e-voting system, whereby the voters, after marking their choice, could see the vote on a ticket behind a glass and, if corresponding, the voter confirmed his or her choice and the ticket was deposited into a box.
6. The possibility for political parties with at least two representatives to nominate an independent IT expert to control the source code and the electoral software; the duties of the IT expert are limited so as not to disturb the workings of the College of Experts.

---

[8] One of the most active groups in Belgium being PourEVA.

[9] Amongst others ECOLO (http://www.poureva.be/spip.php?article138&lang=fr) and PS (http://www.senate.be/www/?MIval=/consulteren/publicatie2&BLOKNR=27&COLL=H&LEG=2&NR=148&SUF=&VOLGNR=&LANG=fr)

[10] The *College d´experts*, created by the *loi du 18 décembre 1998*, is an independent, consultative public regulatory body appointed by both chambers of Parliament for national elections and by regional Parliaments for local ones. It is composed of IT experts and has large legal control competencies (following article 5bis of law 1994 *organisant le vote automatisé*); they have access to both the hardware and software 40 days in advance of the elections and up to 15 days after the elections. On election day, they have access to any polling station. The College of Experts delivers a report within 15 days after each election. There is no legal obligation to publish it although it is normally done.

Since the 2004 European elections, all tests (optical scan, ticketing) were discontinued but the other controls remained in place. A number of proposals for legal amendments have been presented since then, although none of them have been approved. Nonetheless, a resolution from the regional Parliament of Brussels-Capital was adopted in July 2006[11] asking for increased "*transparency to the e-voting system"*.

Following intense reflection on the future of e-voting since 2006[12], the government commissioned an in-depth comparative study on e-voting systems. The proposed solution was a combination of a touch-based e-voting machine and a VVPAT to be scanned by the voter and then inserted into a ballot box.

The study was the subject of a parliamentarian debate in the Federal Parliament in 2008 and, following a resolution[13] enabling the continued experimentation with the e-voting , on July 2008, the Council of Ministers entrusted the Minister of Interior to sign a cooperation agreement with the regions[14] who wanted to participate. An agreement was signed between the Federal Government and the Flemish and Brussels-Capital Regions and a tender[15] was launched by the three administrations for the development of a new e-voting system[16]. As a result of the tender, a 15-year contract was awarded to a consortium led by Smartmatic.

The new e-voting machines were tested on October 27, 2011 in the Flanders and Brussels-Capital regions and will be used for the first time during the next provincial and municipal elections on October 14, 2012.

---

[11] http://www.weblex.irisnet.be/Data/crb/Doc/2005-06/110152/images.pdf

[12] In a response to a written question, the Ministry of Interior announced on May 3, 2006 the creation of a working group in charge of defining the new rules for an e-voting system that will be applied from 2008 onwards and that will have to take into account *"les possibilités de contrôle des opérations de vote par le citoyen et les possibilités de recomptage des votes émis au moyen du vote électronique*". http://www.senat.fr/lc/lc176/lc176.pdf

[13] http://www.lachambre.be/FLWB/PDF/52/1278/52K1278001.pdf

[14] Following a transfer of know-how in 2001 (*Loi spéciale du 13 juillet 2001*), the regions maintained their compentencies for the organization of municipal and provincial elections.

[15] Tender published on September 1, 2008 in the Belgian *Bulletin des adjudications*: *Avis de marché N*. 051333, page: 20459, SPF Interieur. *Développement d'un système de vote électronique*. Published on September 1, 2008 in the Official Journal of the European Union: OJ/S S170. Published on 03 September 2008.

[16] The Tender oversaw the establishment of a 15-year framework contract with several providers. It implied a joint-mixed contract with a majority of services (organized on behalf of the Ministry of Interior and the Regions who would join) but including supplies and had an estimated value of between 75 and 175 million euros.

As for Wallonia, the government wanted to end the actual experimentation of e-voting[17], stating that traditional voting should be promoted and that alternatives to e-voting that offer a paper trail should be examined. In June 2011, the Walloon Government announced[18] the return to traditional voting for the 39 municipalities where e-voting machines had been used, and launched a tender to develop a new e-voting system; that tender is currently suspended. According to the Federal Public Service Interior[19] (FPSI) the aforementioned communes will continue to vote using the current e-voting system.

3 The 2007 BeVoting Study and the 2008 Council of Europe Report

The Belgian federal and regional administrations commissioned a consortium of seven Belgian Universities[20] with the task to make an independent comparative study of different e-voting systems known as the BeVoting study (the Study) [see Ku07]. The Study was tasked with finding the best e-voting system with respect to international standards and the Belgian electoral legislation. That proposal would include the requirements for the new voting system in such detail that the report may serve as a technical appendix to the call for tenders.

The Study, delivered in 2008, is divided into two parts. The first part presents the latest innovations in electronic and Internet voting systems in all aspects (including pros and cons and the costs of different voting systems). It also evaluates the acceptance of e-voting by Belgian voters[21]. The second part proposes five possible e-voting systems[22] and their technical and specific requirements.

From the five systems, the one preferred by the Consortium is called "*improved paper-based voting system*". In this system, the voter casts his vote using a voting computer and the computer prints the vote on a paper ballot that has two parts: a human-readable part and a machine-readable part (a barcode or an RFID chip). Once the vote is printed, the voter verifies that the printed vote is the one he or she has cast and then the voter folds the ballot so that only the machine-readable part remains visible or inserts it into an envelope. The voter then presents it to the president of the polling station to have it inspected for visual marks and then deposits it into the ballot box.

---

[17] http://easi.wallonie.be/servlet/Repository/DPR_wallonne_2009.PDF?IDR=9295

[18] http://www.poureva.be/IMG/pdf/Notification_NGW_-_vote_electronique_090611.pdf

[19] The Federal Public Service of Interior (Service public federal Intérieur), formerly the Ministry of Interior, is a Federal Public Service of Belgium, created in 2002 by Royal Order and in charge, among other things, of Institutions and Population (including the administration of elections). http://www.ibz.be

[20] Katholieke Universiteit Leuven, Universiteit Antwerpen, Universiteit Gent, Université Catholique de Louvain, Université de Liège, Université Libre de Bruxelles and Vrije Universiteit Brussel.

[21] In the report, the consortium concluded that the introduction of e-voting had no significant effect on voting behaviour and that it only reduced the number of blank and invalid votes and also slightly reduced voter turnout.

[22] "*improved paper-based voting system*", "*direct optical scanning*" (based on paper ballots), "*thin-client system*" (e-voting machines connected to a local server using a local network with the possibility to produce a VVPAT), "*Internet/remote voting system*" and "*kiosk voting*".

A report from the Council of Europe (the Report) [see Co08], published in 2008, assessed the overall coherence of the above-mentioned BeVoting study and the compatibility of the five scenarios presented in the Study (and especially of the proposed one) with the recommendations (2004) of the Council of Europe on the legal, operational, and technical standards for e-voting (the Recommendations) [see Co05].

The Report reminds us that none of the scenarios, as presented in the Study, fully comply with the Recommendations, but, following some adjustments to the first scenario ("*improved paper-based voting system*") there should be no problem in complying with the Recommendations. For the other scenarios, more modifications would be required, the Internet voting option being the one which would need the greatest number of legal and security changes.

As for the first scenario, since it is quite similar to the current electronic voting scheme in Belgium, the OSCE considered that it would not require a significant adaptation in the electoral routine of Belgian e-voters under the present system, which is a clear advantage, although it introduces some key changes to both update the technology and to increase transparency.

There were several issues pointed out in the Report that need to be taken into account by the Belgian authorities:

1. Although the Recommendations do not express a preference between the human-readable and the machine-readable part of the vote, the Report signals that from a legal standpoint the human readable part should prevail as it is the only part comprehensible to the voter.
2. The proposal of a non-transparent ballot box, which could go against the transparency of the system.
3. There is a need to strengthen the current audit and certification mechanisms.
4. Officials should re-think the current arrangements when it comes to training.
5. The nature of the physically division of a vote could have legal implications as to which part of the separated vote represents the genuine will of the voter.
6. The fact that the study suggests using a non-transparent ballot box does go against the goals of transparency
7. A detectable amount of radiation was detected from the voting machines.

4 The New E-voting System

The new voting system[23] was developed by a Smartmatic-led consortium that also includes Steria and Wincor-Nixdorf. Specifically customized for Belgium, it is based on the system proposed in the aforementioned BeVoting study.

This new prototype seems to be a combination of the first two systems proposed in the study ("*improved paper-based voting*" and "*direct optical scanning*") and consists of a combination of a touch-based electronic voting machine (17" touch screen SAES3350), a barcode printer, a scanner, and a ballot box (e-urn).

As with the current system, it is the president of the polling station that activates the voting machine with a USB key booting up the equipment. The voting procedure starts[24] with the verification of the identity of the voter by the polling station staff after which the voter is given a token (smartcard) which will allow him or her to activate the voting machine in the voting booth.

Once the voter has chosen and confirmed his or her vote on a touch screen, the machine prints out a ballot containing two parts, a human-readable part and a machine-readable part (a two-dimensional barcode similar to a QR). After verifying that the printed vote is correct, the voter is supposed to fold the paper in two, with the human-readable part on the inside, and take it to the polling station officials, who will inspect it for marks. The voter then goes to the separately located ballot box, scans the barcode on the ballot using the scanning unit, and puts it in the opaque[25], sealed ballot box (e-urn). The scanning unit is connected to a laptop, which automatically stores the vote cast on two redundant, secure USB sticks. The laptop only contains the electoral administration tool used for administering the voting cards and for operating the USB-sticks, nothing else. Linux is the operating system used for the laptops.

The system includes a safeguard so that the screen of the president of the polling station will show the message "*double vote*" and the vote will not be registered[26] should a printed ballot be scanned a second time,

---

[23] http://www.vlaanderenkiest.be/sites/default/files/BeVoting-brochure-belgicav-3.1.pdf

[24] http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/experiment-201110/voteren10etapes.pdf

[25] In its Report [see Co08a pags 6-7], the Council of Europe was against the proposed used of a non-transparent ballot box in the Study [see Ku07b pag 44] as it would clash with the transparency of the system. Nonetheless, the FPSI points out that since the vote is printed in the booklet and an envelope is not used, if a transparent box were used, there could be a risk for the secrecy of the vote if the booklet would open inside the urn.

[26] According to the FPSI, in order to make sure that each barcode is unique, there is a unique key generated and inscribed within the barcode (for each polling station and vote).

The main novelty of the system is that the vote is registered in paper and not in a magnetic card; like that, the voter has the opportunity to verify if the vote has been correctly registered; the voting paper would also serve as a VVPAT in the case of a necessary recount.

4.1 Testing the System

At the request[27] of the Federal Minister of the Interior, the Vice Minister-President of the Flemish Government and the Minister President of the Government of the Brussels-Capital Region decided[28] to organize a large-scale, public, non-binding pilot test[29] on October 27th, 2011, with fictitious candidate lists in order to check the reliability of the new e-voting system under real conditions.

In order to make the test as representative and realistic as possible, the organizers chose a wide range of places and voters to carry out the tests, so that so 6.134 votes were cast in 22 different locations with 90 voting machines[30]; also, the same opening and closing hours for the polling stations as in real elections were applied. Every polling station consisted of a small staff: a president, two assistants, and two observers for a total of 130 election staff (all of them members of the Federal, Flemish, or Brussels administrations). As reported by the FPSI, although some minor issues occurred during the tests (electricity failures, problems with printers and scanners, etc.) most of the reactions from the public were very positive and the only moment where there were doubts was with the scanning since it is a novelty of the system. It also seems as though a large number of voters didn't fold their votes before leaving the voting booth and that they scanned their votes without having them folded[31]. According to the FPSI, this could easily be solved through voter information and training.

As reported by the FPSI, the presidents of the polling stations declared that "*the public finds the system simple and easy. There have been small technical problems, but we can say that the experience has gone very well.*"[32] Erwin Hertens, from the FPSI, declared that "*this is excellent! With all my heart thank you to all those who have done this for us on a voluntary basis. We can say that the system has really been tested from every angle, and we have now to review all comments and to make a deep evaluation.*"[33]

---

[27] http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/experiment-201110/Com-presse-experience-systeme-vote-electronique-241011.pdf

[28] The Minister of Interior at that time, Annemie Turtelboom, declared that before the different administrations decided to purchase the system, they wanted to test the e-voting machines in real conditions (http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/experiment-201110/Com-presse-experience-systeme-vote-electronique-241011.pdf)

[29] http://www.experience2011.rrn.fgov.be/fr/

[30] http://www.ibz.rrn.fgov.be/index.php?id=3011&L=0

[31] Ibid

[32] Ibid

[33] Ibid

This recently tested prototype is meant to replace the old machines and is supposed to be used for the first time in the next Belgian provincial and municipal elections in October 2012[34], in 149 municipalities in the Flemish Region and 2 municipalities in the Brussels-Capital Region.

5 Analysis of the New System

As has been repeatedly pointed out, in e-enabled elections it´s not possible for everybody to understand the system, and therefore voters need to rely on others who are in a position to understand the IT materials and the processes. Therefore, it's very important that the election administration is as transparent as possible. This transparency will contribute to the voter´s knowledge and understanding of the voting system. Introducing auditable measures like a second storage medium which provides physical, unalterable evidence of how the voters voted can help to increase transparency and a voter's trust in the system.

Consequently, the introduction of a human-readable part in the new Belgian e-voting system implies a clear improvement with regards to the transparency and verifiability of the electoral procedure, since the new ballots would serve as a VVPAT and would allow for audits and recounts and could also be used as a potential backup in case of a system crash. All this would potentially increase voter trust and confidence in the Belgian e-voting system.

On the other hand, it should be noted that several issues still remain open. Among them, several important topics that are consistently addressed both by the Council of Europe and OSCE when dealing with e-voting systems:

- Transparency: According to the Council of Europe, in order to increase transparency, it is essential that stakeholders have as much access as possible to relevant documents, meetings, activities, etc. PourEVA states that the prototype used computers dedicated for this single purpose and used proprietary code. According to the FPSI the voting software will work with Linux and the source code will continue to be made publicly available.
- Secret suffrage: It is one of the basic principles of democratic elections. This implies that when implementing e-voting systems, assuring that the link between the identity of the voter and vote itself is permanently removed.

With this new system, as with the previous one, this would seem in principle to be guaranteed since the identification and authentication phases are separate from the voting one.

[34] Provincial and municipal elections (*Elections provinciales et communales*) to be held in the 3 regions of Belgium on October 14, 2012. The regulation and organization of provincial and municipal elections is an exclusive competence of each of the three regions in Belgian.

Although it appears from the tests of the new system that some voters don´t fold their paper votes (which could endanger the secrecy of their votes), the FPSI notes that to solve this issue, an information and training workshop needs to take place in order to make the voters familiar with the new system.

On the other hand, according to PourEVA, there is a potential danger to voter privacy if on election day a ticket cannot be scanned (due to an IT bug, a problem with the printer, etc.) and the voter needs assistance from the election staff, they could know the sense of the vote of that particular voter. According to the FPSI, in a case like this, the vote is cancelled and the voter can vote again. Furthermore the polling station staff is responsible, under oath, for guarding the secrecy of the vote (with financial and criminal sanctions possible for the polling station heads that don't comply).

Finally, there may remain some potential danger (common to every IT system) of electromagnetic radiation that could infringe upon the secret suffrage by allowing others to see what information the machine is managing, printing, or receiving. This was already pointed out by the 2008 Council of Europe Report [see Co08a pag 4] and in this respect PourEVA questioned[35] whether all machines were tested against this kind of attack and if they will be for every election. According to the FPSI, a scientific study has determined that the voting machines are in accordance with the requirements of the NATO Zone 1[36] and that furthermore, since the polling stations are composed of 5 voting machines, the radiation from the computers would mix.

- Machine-readable/human-readable part of the vote: The Council of Europe [see Co10a pags 10 and 11; Co10c pags 11, 12 and 22] states that when introducing a paper trail, arrangements have to be made to deal with any discrepancy that may arise between the machine- and the human-readable part of the vote; clear rules should be implemented to determine which type of vote takes precedence. The Council of Europe Report [See Co08a pag 5] pointed out that although the Recommendation does not express a preference between the barcode or the ballot booklet inserted in the ballot box, from a legal standpoint the human readable part should prevail as it is the only part comprehensible to the voter.

According to the FPSI there is still no legislation related to the new e-voting system, since the next elections organized by the federal government will normally take place in 2014.

[35] http://www.poureva.be/spip.php?article701

[36] According to the TEMPEST Standards, the NATO SDIP-27 Level B and USA NSTISSAM Level II ("Laboratory Test Standard for Protected Facility Equipment") is a standard for devices that are operated in NATO Zone 1 environments, where it is assumed that an attacker cannot get closer than about 20 m (or where building materials ensure an attenuation equivalent to the free-space attenuation of this distance).

On the other hand, PourEVA noted[37] that with the new system the voter cannot verify that the vote registered in the machine-readable part corresponds to the one in the human readable part (PourEVA had already criticized[38] that the optical reading system was rejected in the BeVoting study without convincing arguments, arguing that optical reading is a system that offers more control by the citizens and had been declared "reliable and mature" by The College of Experts[39]). According to the FPSI, there will be a booth at the polling stations where, with the assistance of a barcode reader and a computer, the voters will be able to scan their votes in order to double-check that the human-readable and machine-readable part of their votes do indeed correspond.

- Audit and certification: The Council of Europe [see Co05 pags 11, 15, 19, 20; Co10a pags 9 and 14; Co10c pags 11 and 51] and the OSCE [see Os06 pag 5, 9; Os07 pag 12-14 and 23] point out the importance of establishing both audit and certification procedures. Auditable systems play a fundamental role in e-voting, and using paper trails in combination with a mandatory count of paper votes in statistical randomly selected polling stations is an excellent way to bolster trust in the system. Certification should be carried out by an independent body in the most transparent way possible, covering all aspects of e-voting and should serve to verify independently that an e-voting system complies with all the specifications and requirements established.

Regarding the audits, although the Study [see Ku07 pags 12, 16 58, 62 and 66] previews that "*independent auditors can select a random set of ballot booklets to audit elections by confirming that the barcode of these randomly selected ballots corresponds with their human readable part*" and one of the strengths of the new system is that it would allow for random audits, there is still no federal legislation concerning the new e-voting system (according to the FPSI this will in principle be done for the 2014 elections).

As for certification, according to PourEVA[40] there is no electoral law or regulation describing the characteristics of the prototype for the new voting system against which the certification company could check and certify it. Furthermore, PourEVA noted[41] that the certification of the new system carried out by PwC remains secret.

Even though there seems to be no specific regulation describing the characteristics of the prototype, it should be noted that the new system has been submitted for certification, according to specifications, with an independent company: PriceWaterhouseCooper. A positive report with regards to the system was submitted by PwC in December 2011. In a Parliamentary debate, Ms Jöelle Milquet (current Minister of Interior) replied to a question[42] that the above-mentioned report stated that "*Based on the activities carried out by us, we can say with reasonable certainty that the software is compatible with the*

[37] http://www.poureva.be/spip.php?article692
[38] http://www.poureva.be/spip.php?article513
[39] http://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=50332887&LANG=fr
[40] http://www.poureva.be/spip.php?article698&lang=fr
[41] http://www.poureva.be/spip.php?article701&lang=fr
[42] House of Representatives. Commission of Interior. Meeting of 18 January 2012. (CRIV 53 – COM 0366) http://www.lachambre.be/doc/CCRI/pdf/53/ic366.pdf

hardware available and for the defined scope, the prototype provided in the tender and the application are suitable"; in that debate she also agreed to transmit the certification report to the parliamentarians who requested it.

- Election observation: the Venice Commission [see Ve02 pag 11], the Council of Europe [see Co05 pags 35 and 36; Co10a pag 6; Co10c pag 40] and the OSCE [see Os06 pag 9; Os07 pag 7; Os08 pags 2, 4 and 14] strongly recommend the establishment of legal provisions to allow election observation. This observation should be effective and include, to the extent permitted by law, presence in polling stations and data processing sites and access at all levels to documentation and reports, including minutes, certification, testing, and audit reports, etc. (respecting the principle of non-interference with the administration of the election). Election observation should include international, domestic, and long-term observation.

At the moment, there does not seem to be specific provisions concerning election observation for e-voting, especially in regards to the new system.

Bibliography

[Be10] Ben Anchour, R.: Etat de la question. Quel avenir pour le vote electronique en Belgique?. A. Poutrain, 2010
http://www.iev.be/getattachment/8d9066d0-5809-4b54-8add-1a9e718dcc3c/Quel-avenir-pour-le-vote-electronique-en-Belgique-.aspx

[Co05] Council of Europe: Legal, operational and technical standards for e-voting. Council of Europe, 2005.
http://www.coe.int/t/dgap/democracy/activities/key-texts/recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

[Co08a] Council of Europe: Compliance of the BeVoting Study with the Recommendation (2004) 11 of the Committee of Ministers of the Council of Europe to the member states on legal, operational and technical standards for e-Voting. Strasbourg, February 2008
http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/Compliance_Belgian_BeVoting_Rec_1_0_final_18_02_08.pdf

[Co08b] Council of Europe: Meeting to review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Strasbourg, 2008.
http://www.coe.int/lportal/c/document_library/get_file?uuid=9c7dec0f-3dde-4024-ae77-e4d6ab6033c2&groupId=10227

[Co10a] Council of Europe: Guidelines on transparency of e-enabled elections. Strasbourg, 2010
http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf

[Co10b] Council of Europe: Evolution du vote électronique en Belgique: le temps de la transition. Strasbourg, 2010
http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/e-voting%202010/biennial_nov_meeting/GGIS(2010)8_Belgique%20e-voting%20report%20F.asp

[Co10c] Council of Europe: E-voting Handbook. Key steps in the implementation of e-enabled elections. Council of Europe. Strasbourgn, 2010
http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf

[Fr07] French Senate. Les documents de travail du Sénat. Série Legislation comparée. Le vote électronique. Nº LC 176.
http://www.senat.fr/lc/lc176/lc176.pdf

[Ku07a] KU Leuven et al: BeVoting. Study on Electronic Voting Sistems. Part 1
http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf

[Ku07b] KU Leuven et al: BeVoting. Study on Electronic Voting Sistems. Part 2
http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-2_gb.pdf

[Os06] OSCE/ODIHR: Local Elections Kingdom of Belgium. 8 October 2006. Expert Visit on New Voting Technologies Report. OSCE/ODHIR
http://www.osce.org/odihr/elections/22450

[Os07] OSCE/ODIHR: Belgium Federal Elections 10 June 2007. OSCE/ODIHR Election Assessment Mission Report. Warsaw, OSCE/ODIHR.
http://www.osce.org/odihr/elections/belgium/28213

[Os08] OSCE/ODHIR : Discusion paper in preparation of guidelines for the observation of electronic voting. Warsaw, 2008.
http://www.osce.org/odihr/elections/34725

[Ve02] Venice Commission: Code of good practice in electoral maters. Guidelines and explanatory report. Strasbourg, European Commission Democracy Trough Law.
http://www.venice.coe.int/docs/2002/CDL-AD(2002)023-e.pdf

[Ve04] Venice Commission: Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe. Strasbourg, European Commission Democracy Trough Law. http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.pdf

The Implementation of E-voting in Latin America: The Experience of Salta, Argentina from a Practitioner´s Perspective

Guillermo Lopez Mirau, Teresa Ovejero, Julia Pomares

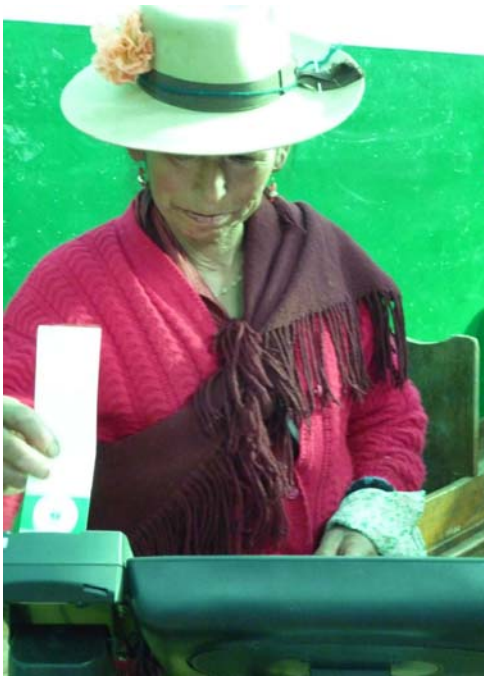
CIPPEC Foundation
Callao 25, 1,
1425 Buenos Aires, Argentina
jpomares@cippec.org

Abstract. The most important implementation of e-voting in Argentina so far took place in the province of Salta, in the north of the country on the border with Bolivia. With an electoral roll of 850,000 voters that is ethnically diverse and a complex electoral geography due to a high percentage of mountainous area, its implementation is very valuable for a comparative analysis. The gradual implementation allowed for a systematic assessment, conducted by a large survey of voters and poll workers, who had used both voting methods (the traditional one and the new voting system). This paper presents this case study, emphasizing the goals pursued by this reform as well as some findings from this large undertaking. It concludes by documenting the lessons learned and examining the challenges ahead.

1 Introduction

Argentina is a federal country with a decentralized election administration system. Each of the 24 districts of the country (provinces) has the power to issue its own electoral system, from its institutions of election administration to the design of electoral rules. Since the enactment of universal suffrage, voting procedures have taken the form of the French ballot and envelope system. In national elections, each political party has its own paper ballot and is responsible for the printing and distribution of the ballots on Election Day. In the last three national elections, this voting procedure was heavily criticized. The main reason, among others, is that the high fragmentation of the party system makes it very difficult to ensure that all political parties have their electoral supply in each polling place. A system originally designed for a two-party system has had problems adapting to the current political system. Therefore, several provinces began to make changes to the voting procedures in provincial elections. Beginning in 2003, different experiences with electronic voting took place across the country as well as the use of a single-ballot system (having all election options on only one paper).

The most important e-voting experience to have been implemented in Argentina took place in the province of Salta, in the country's North on the border with Bolivia. It has approximately 1,200,000 inhabitants and has an electoral roll of 850,000 voters. Its electoral administration becomes complex because it has a high percentage of mountainous area. Some of the locations, currently only accessible by mule, still do not have basic services like electricity. In addition, Salta is one of the few Argentine provinces that has a lot of ethnic diversity: 10% are descendants of native peoples. Picture 1 shows an indigenous woman casting her vote, and picture 2 shows the village of Nazareno in the province of Salta, the first place where e-voting was tested.



Picture 1: an indigenous woman casting his vote in Nazareno, Salta, 09/08/2010
Picture 2: view over Nazareno, Salta, 09/08/2010

The e-voting implementation in the province of Salta began in 2009 and will conclude in 2013 once the system has been expanded to 100% of its electoral roll. It has important implications for the rest of Argentina and the region. The gradual implementation has allowed a systematic evaluation of the impact of changing voting procedures on voters and the political parties. Currently, several provincial legislatures are examining the possibility of reform projects to change voting procedures and the experience in Salta provides systematic evidence to this debate.

This paper aims to present this experience, emphasizing the goals of the reform as well as some findings from an evaluation carried out by the Government of Salta, the Electoral Court, and the Center for the Implementation of Public Policies Promoting

Equity and Growth (CIPPEC), a think tank based in the city of Buenos Aires. First, this paper describes the characteristics of the implementation of electronic voting in Salta. It describes the context in which it has been deployed and system characteristics (section 2). Section 3 identifies the objectives sought by the provincial executive by implementing this e-voting system. Section 4 presents some conclusions of the evaluation, and section 5 concludes, emphasizing the lessons learned and challenges ahead.

2 Characteristics of the Implementation of E-voting in Salta, Argentina

In 2004, the Electoral Court of the province of Salta[1] started to evaluate the possibility of incorporating new information and communication technologies into the electoral process. When the government of Salta decided to implement new technologies into the electoral process, it sent a bill to the legislature to amend the provincial electoral system. The law was passed in late 2008 with very general provisions, giving the Provincial Electoral Court the authority to approve and control the electronic voting system and to ensure that the technical information was passed on to all political parties. The legislation does not provide specific regulations on how to audit the e-voting system.

The electronic voting system chosen by the province[2] is provided by a private company in Argentina and has a fundamental characteristic: the information is stored on the ballot and not inside the voting machine. In fact, it is a machine which allows the voter to create, in the actual sense, her vote. The design of the ballot has a similar design to the traditional paper ballot but also incorporates a chip which electronically records the will of the voter. This system maintains the use of the ballot paper and the ballot box but adds technology to the process of voting and tallying.

The following explains the steps needed to cast a vote with the voting machine: First, the voter shows up to the poll authorities and hands them her ID. Then, the authority verifies the data on the roll. Assuring she is eligible to vote, the poll authority provides the voter with an e-ballot and invites her to approach to one of the voting machines. The voter inserts the ballot into the printer's slot of the machine. Using the touch screen, she chooses the parties or candidates by simply touching the appropriate field. The system allows voters to either cast a straight ticket or a vote for a different party in each race. When finished, the display provides a summary of the ballot. The voter must "confirm" or "go back" as desired. If confirmed, the choice made by the voter is printed on the ballot as well as recorded in digital form onto the incorporated RFID-chip. To verify that the printed information is the same as the information on the chip, the voter places the ballot with the printed side up on the verifier. The information recorded on the chip appears on the screen and is identical to the printed information on the paper. Finally, the

[1] According to the constitution of the province, this body is empowered to arrange the organization and functioning of the election.

[2] The legislation does not specify a type of election system that has to be used. It was defined by the executive of the province in accordance with the Provincial Electoral Court.

voter must fold the ballot (with the vote inward), go back to the table, put the ballot into the ballot box, and collect the signed and sealed document of identification from the polling authorities. Pictures 3 through 5 show the voting machine and the e-ballot.

Picture 3: Voting Machine

Picture 4: an elector inserts her ballot paper in the voting machine

Picture 5: printed ballot paper close to the verifier

Once the election is closed, the tallying of the votes begins (provisional tally of results). The functionality of the machine is changed from “voting machine” to “tally machine”. To do this, the poll authority has an identification card, with an RFID chip, that enables the system by holding it close to the verifier of the machine. In the menu, she chooses "Close Election and Tally Results". The next step is to open the ballot box and one by one, take the votes and pass them through the reader of the machine. The system shows, visibly on the screen and by making a sound, the advance of the reading process and of the sum of the votes. If the ballot is read correctly, one hears a "beep" specific to that condition and "Reading OK" appears on the screen. Scanning a vote more than once, causes the message "repeated vote" to appear, and the vote is discarded. If the electronic ballot (BUE) could not be read, the display indicates this circumstance and discards it. This BUE will be classified in the category of "provisional ballot" and later, during the final counting process, the electoral court will decide its validity.

Having read the last vote, the results of that voting table are displayed. Pressing "Finish Scrutiny" the system asks the poll authority to enter the number of "provisional ballots". Those figures, together with the results, will be printed on the closing minutes and on the certificate of transmission. This certificate transmits the results of this table to the computer center.

The introduction of the system began shortly after the enactment of the law in 2008, which allowed the gradual implementation of an electronic voting system. Partial implementations took place in 2009 and 2011, both in general elections and in the open primary process established by provincial legislation. The first experience with electronic voting in the province of Salta was during the elections of 2009. In both elections, the open and simultaneous primary elections that took place on July 12, 2009, as well as in the general elections of September 27 of that year, a pilot test was conducted using the system described above. The test was binding and was conducted in both elections in a town near the provincial capital (San Lorenzo), with 9200 voters. In the general election, 11 voting tables (4191 voters) in the capital of Salta also used the electronic ballot system.

During this pilot test, a survey was taken with a sample of 410 voters. The results showed some preliminary positive perceptions of the system and provided guidelines for the dissemination of e-voting in further elections. According to the survey, the voters found the system easy to use: 36% said it was easy and 57% said it was very easy to vote, while the negative opinions did not exceed 7%. The study also showed positive opinions regarding the confidence in the new system. 7 out of 10 respondents said they could rely on the new system more so than the previous system.

As a consequence of the satisfactory performance in the 2009 elections, in the general election on April 10, 2011, 33% of the registered voters in the province of Salta could vote with the electronic ballot voting system. The election was carried out in 50% of the electorate of the municipality of Salta, and all the municipalities of San Lorenzo, La Caldera, San Ramon de la Nueva Oran, San Jose, Metán and Cafayate. In total, 244,702 voters were able to vote with the electronic ballot voting system (distributed throughout 79 polling stations). The next section delves into why this voting system was introduced.

3 The Goals Pursued by the Reform

According to the executive decree specifying the required characteristics and conditions of the e-voting system, the reform introduced by the government had several objectives. Here we emphasize the objectives that are more valuable for a comparative analysis of this experience. First, the reform aimed to increase the voter's confidence in the voting system. Second, the introduction of e-voting sought to increase the speed of the vote count. In contested elections, a long process of tally of results can create uncertainty and mistrust, especially among political parties. Third, the voting procedure chosen was designed to give the voter the possibility to easily vote in individual races or by party. As mentioned above, in the national voting system the voter needs to use scissors to cut out the various paper ballots of different parties in order to vote for a different candidate in every race. In other words, the default option is a straight ticket vote. The e-voting system made the preference for a candidate rather than for a political party easier than the traditional method, although it maintained an option of straight ticket vote. A thorough assessment of the achievement of these three goals would require a longer timeframe but there is some preliminary evidence concerning the performance of the new voting system at the 2011 elections that supports the conclusions that the implementation might have achieved the aforementioned goals. The next section presents the preliminary evaluation of the new system's impact on the confidence in the election process. In the remainder of this section we provide some evidence on the performance of the new system with regard to the other two issues: increasing the speed of vote count and allowing for a split ticket vote.

The second objective, to speed up the vote tallying procedures is also associated with trust in the election process. In the context of volatile perceptions of trust in election processes and contested electoral results, delays in obtaining the results could produce social uncertainty and affect the legitimacy of the election process. E-voting mitigates this by increasing the celerity of the vote-counting process. This goal was clearly achieved in the 2011 elections when one-third of voters used the electronic voting system and two-thirds voted manually. The electronic voting system marked a drastic improvement in the speed of the counting process, the preparation of the minutes, and the scrutiny in general. During the first two and a half hours after the official closing of the polls (6 pm), the results received were almost only those from the precincts that had used the electronic voting system (see Figure 1 below).

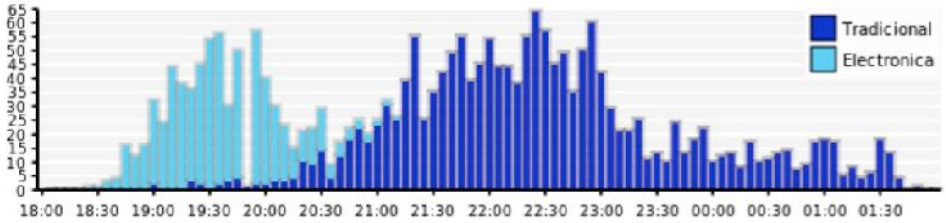


Fig. 1: Histogram of Number of polling tables' tally of votes received by the Electoral Tribunal by type of voting system, source: Electoral Court of the province of Salta

A third important aspect of the implementation of e-voting devised by the provincial executive government has to do with allowing a split-ticket vote. In the context of a highly fragmented party system [CE05], there is anecdotal evidence that voters have become more independent and less partisan in their electoral choices over the last decade. Against this backdrop, the e-ballot system implemented in Salta plays a key role in facilitating a split-ticket vote. As mentioned above, the voter has the option of voting for the entire list of candidates of only one party or voting for a different candidate in each race by touching the screen. In contrast, in the case of a traditional paper ballot system, the elector has to cut various paper ballots to mix his choice of candidates, which can be confusing and, if not done correctly, could nullify the vote.

According to the survey, the percentage of split-ticket voting is significantly higher among e-voters in comparison to traditional voters in the 2011 elections. While approximately 50% of voters using the electronic voting system said they split their ticket, in the traditional voting system only about 25% said they voted for different parties in each race. As expected, the individual votes per race were mainly cast by younger voters.

Voters were also asked whether they preferred cutting out the traditional paper ballot by hand or splitting the ticket electronically. The question aimed to determine the degree of discomfort that may cause a voter to vote using the traditional system. Almost 8 out of 10 voters who used the new voting system preferred to split the vote electronically. Even a majority of voters of the traditional system indicated their preference for the electronic system to split a ticket (49.9%) while 43.4% preferred to cut out their votes manually.

These figures might indicate that the chosen system makes a split ticket easier. Although this finding may provide evidence that one of the goals of the reform was accomplished, this fact should not be equated to an increase in the quality of the party system. The case could be made that this voting technology could only reinforce party system fragmentation trends. Further analysis is required on this issue.

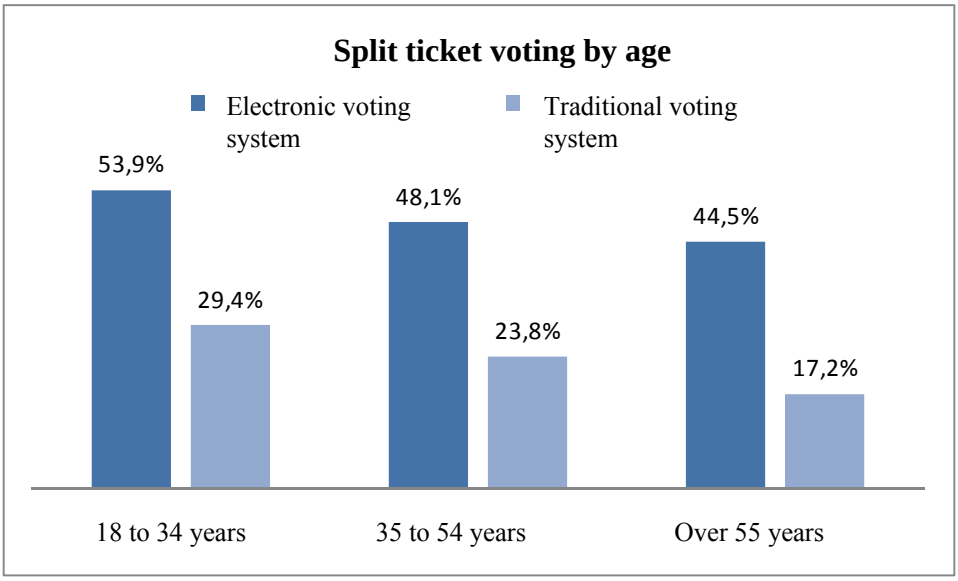


Fig. 2: Percentage of split-ticket voters using and their voting methods, broken down by age "Which voting method of voting did you use in today´s election?", Source: survey of 1502 voters

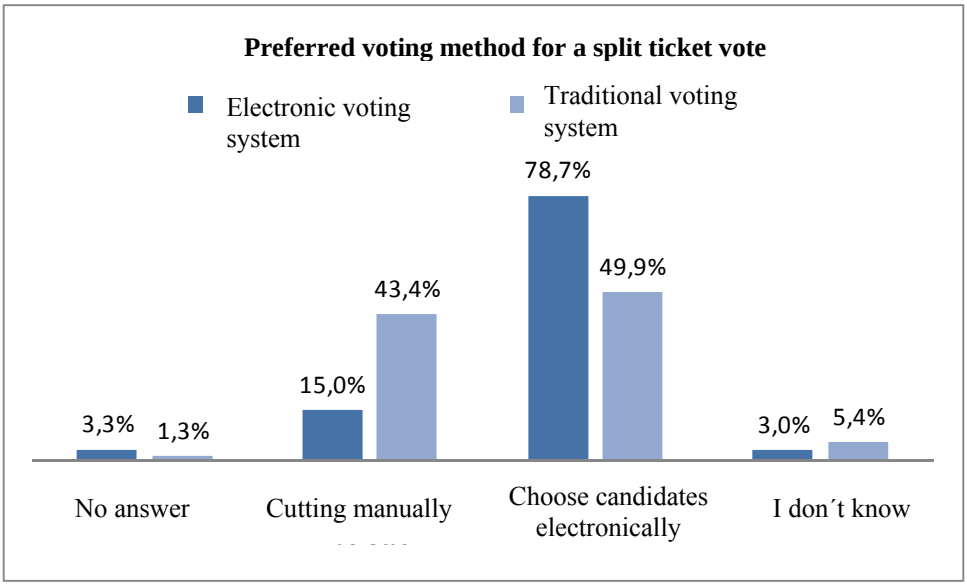


Fig. 3: Preferred method for voting a split ticket. "If you wish to vote for candidates of different parties, which voting method do you prefer?
Source: survey of 1502 voters

4 Some Findings from the 2011 Evaluation

During the election of 2011, together with the think tank CIPPEC, a major effort was made to evaluate the implementation of electronic voting in Salta. The partial implementation of the new system in the province of Salta provided a unique opportunity to carry out a systematic and rigorous comparison of the e-voting system with the paper ballot voting system (hereafter the "traditional" method). To gage the level of support and overall satisfaction with the new voting procedure among voters, poll workers, and political parties, a research team employed quantitative techniques (a survey of perceptions and opinions of voters and poll workers) and qualitative techniques (participant observation and interviews with election officials and leaders of political parties).

On election day, a total of 1,502 voters and 112 poll workers were questioned about their perceptions and opinions of both types of electoral systems; both, in voting sites using the traditional system and in voting sites using the e-voting ballots. Also, 18 leaders from 13 provincial political parties and electoral alliances were surveyed. The evaluation covered a large range of questions and issues but two aspects are discussed here in detail[3]. We analyze the impact the new system had on overall support and on the confidence of voters and political parties. Also, we mention some perceptions of political parties' leaders on the consequences of changing voting procedures over their strategies in electoral campaigns.

As indicated by the surveys, the vast majority of voters and the poll workers that used the electronic system, preferred the new system rather than returning to the previous system. Most people using the traditional system (even though it was a smaller majority) would have preferred the electronic alternative. Therefore, the replacement of the traditional voting procedure has full the support of voters who tested the electronic voting as well as of those who voted with the traditional system.

An important component of the evaluation has to do with the impact of the new voting procedure on confidence in the election. There are several definitions of this component. For the purposes of this paper, our starting point is the view presented by Giddens, who analyzes trust in his study of the consequences of modernity [Gi90]. He differentiates between trust and confidence by arguing that trust is a specific type of confidence mediated by faith and, hence, by contingency. He defines trust as 'confidence in the reliability of a person or system, regarding a given set of outcomes or events, where that confidence expresses a faith in the probity or love of another, or in the *correctness* of abstract principles (technical knowledge)' [Gi90, p. 34, emphasis added]. Abstract systems engaged in election processes need to guarantee that their correctness is *fair*. Trust in the election process entails trust in the *impartiality* of state institutions.

Beyond the broad concept of confidence, there is a need to break it down into different components [Po11a]. We focus on two different aspects: the perceptions that the vote is properly stored and counted and the confidence in protecting the secrecy of the vote. The first aspect is related to the system's ability to correctly translate the expression of the voters' will and the second is related to the secrecy of her choice. Different questions

[3] For a thorough analysis of the findings of the study, we refer to [Po11b] and [AL12].

were asked for each voting system. Voters who used the electronic voting system were asked how secure they felt that their vote was correctly registered. The voters using the traditional system of counting were asked how secure they feel that their vote had been correctly counted.

It was found that both voting systems are perceived as reliable and safe: 6 out of 10 voters in both systems were sure that their vote was counted correctly (see Figure 4 below). 83.1% of voters that used electronic voting reported feeling "confident" or "very confident" that their vote was registered correctly. A statistical analysis carried out using a matching method showed that the impact of this technology clearly increases this dimension of the confidence of the voter [AL12].

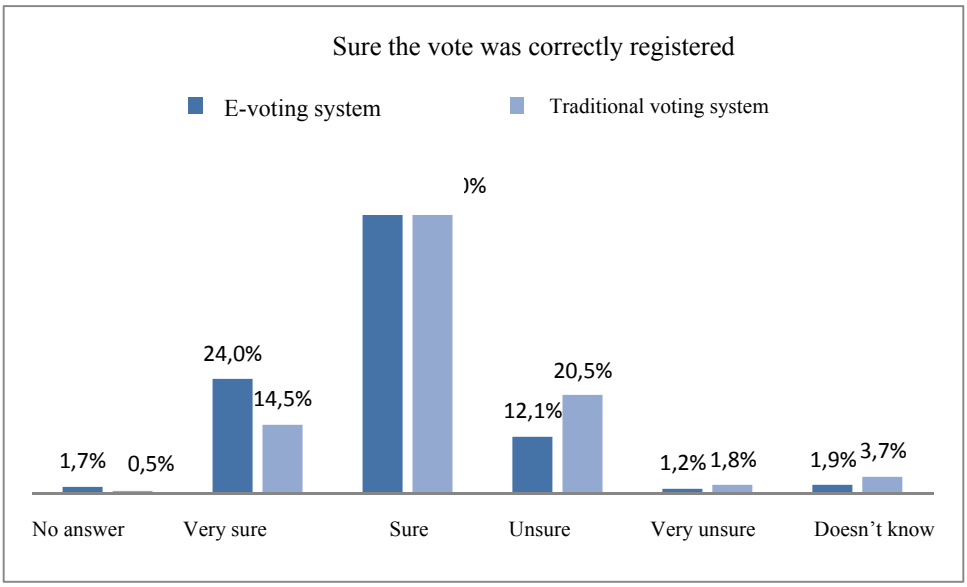


Fig. 4: Answers to questions "Are you sure your vote was correctly registered?
By voting system, Source: survey to 1502 voters

The confidence in the secrecy of the vote was found to be high in both systems, although slightly higher among voters using the traditional method. While 74% of the e-ballot voters said they were "confident" or "very confident" that their vote was secret, among the traditional voters the figure was 83%. The statistical analysis confirms the small but negative influence of the new technology on the confidence in the secrecy of the vote. It is not easy to draw conclusions about the reasons behind this impact. It may be due to the particularities of traditional voting in Argentina. The ballot and envelope system used in Argentina implies that the voter enters a closed room alone where she casts her vote without being observed or making eye contact with others. By contrast, the electronic voting system (like any e-voting system) is operated at a short distance from the table and the voter can see and be seen from behind the voting booth.

Empirical investigations into the sources of confidence in elections are conducted almost exclusively from the perspective of voters rather than that of political parties, even though, if 'the dynamics of politics is in the hands of losers,' as Riker [Ri83] puts it, it is at first place in the hands of political elites [EMR08]. Since the voting system must be reliable both for voters and for political parties, the evaluation also captured the perceptions of political party members. Interviews with leaders and members of political parties show that an important element of trust in the new system is that the chosen system maintains the paper ballots and the ballot box. Party members supported the new voting system although their leaders expressed some concerns. These concerns are mainly due to the fact that the new system seems to defy the ability of parties to adapt the control routines of elections which they had developed for the previous method. Also, according to interviews with party members, the absence of audit mechanisms in the normative framework is perceived as a weakness of the reform.

5 Conclusion: Policy Lessons from the Salta Experience

This paper aimed to present the experience of e-voting in Salta, Argentina. It is the most important e-voting experience implemented in Argentina so far and the gradual implementation of the e-voting system allowed for a systematic evaluation of the perceptions of voters and poll workers about the new voting system. The voters' survey shows that the electronic voting system is supported by most voters and poll workers and there is an overall consensus about the support for a change. The e-voting system also increases confidence in the ability of a correct translation of the electoral will into a vote. Voters are also confident in the secrecy of the electronic vote. However, this dimension of trust, the traditional method of voting performed better than the electronic voting system. This might be transitional, but it also points to the importance of training and communication efforts. Due to the fact that the gradual implementation at 2011 elections focused on polling precincts with better telecommunications infrastructure, the proportion of highly-educated voters was higher than the provincial average. Therefore voters training and communication strategy should be further enhanced in the total rollout for the 2013 elections.

The evaluation also shows that the e-voting system facilitates split-ticket voting, giving greater prominence to the candidate over the political party. The voting procedure seems to reinforce a pre-existing trend and there is a challenge ahead that has to do with analyzing whether the new system would further fragment the party system and its cohesion. Finally, the experience of Salta confirms the advantages of a gradual approach to the roll-out, which allowed for adjustments to be made throughout the process and resulted in a better implementation of a new voting procedure.

Bibliography

[AL12] Alvarez, R.M., Levin, I., Pomares, J. & Leiras, M., 2012. The impact of e-voting on citizen perceptions and opinions. *Manuscript*.

[CE05] Calvo, E. & Escolar, M., 2005.*La nueva política de partidos en la argentina: Crisis política, realineamientos partidarios y reforma electoral*: Prometeo.

[EMR08] Estévez, F., Magar, E. & Rosas, G., 2008. Partisanship in non-partisan electoral agencies and democratic compliance: Evidence from mexico's federal electoral institute. *Electoral Studies 27,* 27, 257-271.

[Gi90] Giddens, A., 1990. *The consequences of modernity* Cambridge: Polity.

[Po11a] Pomares, J., 2011. Inside the black ballot box. The origins and consequences of introducing electronic voting. *PhD Dissertation.* London School of Economics and Political Science.

[Po11b] Pomares, J., Leiras, M., Chintian, C. & Peralta Ramos, A., 2011. Cambios en la forma de votar. La experiencia de salta con el voto electrónico. *Documentos de Políticas Públicas.* Buenos Aires: Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento, CIPPEC.

[Ri83] Riker, W.H., 1983. Political theory and the art of heresthetics. *In* Finifter, A.W. ed. *Political science: The state of the discipline.* Washington, DC: American Political Science Association.

Session 8

Analyzing E-voting: Surveys and Results

Mapping the Literature: Socio-cultural, Organizational and Technological Dimensions of E-voting Technologies

Nina Boulus-Rødje

Technologies in Practice Research Group
IT University of Copenhagen
Rued Laanggaardsvej 9
2000
nbou@itu.dk

Abstract: As the utilization of various e-voting technologies has notably increased in the past few years, so has the amount of publications on experiences with these technologies. This article will, therefore, map the literature while highlighting some of the important topics discussed within the field of e-voting. Particular attention will be paid to the non-technical dimensions of implementation, including the socio-cultural, organizational, and political dimensions.

1 Introduction

The recent popular uprising in the Middle East has given us the possibility to witness how technology (i.e., social media) can be used as a strong weapon for democracy. However, when it comes to e-voting technologies, it remains unclear as to whether they are encouraging or discouraging democracy. E-voting technologies are imagined as having the capacity to do a wide range of things: increasing overall voter turnout, increasing the efficiency and accuracy of the electoral process, as well as reducing waiting time and costs. Such idealistic visions are familiar from other domains, for example, the field of healthcare, where similar rhetoric can be heard regarding the implementation of Electronic Patient Records (EPRs).

In both fields, we find that some of the visions are disputed (e.g., saving costs and increasing efficiency). The great difference, however, is that there is a general agreement that implementing EPRs is a goal that all healthcare institutions should strive to achieve. However, with e-voting technologies we still find ambiguous messages from both politicians and scientists, expressing reservations toward procedural and technical aspects. One of the main concerns is that these technologies "black box" the electoral process, removing current public control and accountability mechanisms and making the process inaccessible for verification. In contrast to the implementation of other technologies (e.g., EPRs), mistakes made by e-voting technologies cannot be compensated and these can have devastating consequences on our democracy.

Although the field of e-voting is relatively young, it has been advancing rapidly and so has the number of issues that have been brought to the table. E-voting technologies have been introduced in new countries and with regards to different types of elections. The literature has been growing and we have more real-life, practical experiences to draw upon. In order to have a better overview of the current state of knowledge and to identify areas requiring future research, this article will map out the literature highlighting some of the main topics discussed within the field.

Recently, there has been greater focus on not only technical dimensions (e.g., hardware, software, cryptographic methods and protocols, and certification and evaluation systems), but also on the socio-cultural, organizational, and political dimensions of e-voting. Particularly, there has been greater focus on the impact of a voter's demographic attributes has on confidence in the electoral process and the e-voting technologies [e.g., Al09b; Cl08; GH09; SAH10]. Most studies that focus on non-technical dimensions draw upon Election Day voting experiences, and almost all studies draw upon quantitative research methods (i.e., statistical analysis of survey data). Collecting data on individual voting experiences is a very recent practice amongst e-voting researchers [SAH10].

This article begins by listing briefly some of the expectations behind e-voting technologies and compares them to the research findings thus far. This will be followed by section 3, which synthesizes and maps some of the main topics discussed in the literature, particularly within studies that focus on non-technical issues. This literature review is divided into two main sub-sections, where the first one (3.1) focuses on the medium, the actual e-voting technology. The second sub-section (3.2) focuses on dimensions that are beyond the medium, including voters' trust in e-voting technology, voters' trust in the electoral machinery, and the influence of other relevant stakeholders. This will be followed by section 4, which discusses the studies presented above and where I propose a typology that distinguishes between findings that are context dependent and findings that are (systematically) repeated across different contexts, allowing them to be generalized to a certain extent. In other words, while section 3 synthesizes and maps the different specific topics discussed across the research projects, section 4 provides a typology, a broader, general map classifying and clustering the different topics into more general themes. Finally, a few concluding remarks will be made regarding the current state of our knowledge of e-voting projects, followed by directions for further studies.

2 E-voting Technologies: Expectations and Status Quo

When reviewing the media and policy discourses surrounding e-voting technologies, we quickly find that the transition from a traditional paper-based voting system to e-voting technologies is often viewed as necessary and inevitable [Ca06]. Although the idea of electronic voting is not new, the implementation of e-voting technologies has turned out to be an unexpectedly long and challenging process, in which many of the goals have yet to be met. Furthermore, the possibility of reaching some of these goals has been

questioned or problematized. Nevertheless, expectations are high and so is the amount of money being spent on the different e-voting projects in several countries.
E-voting technologies are expected to improve accessibility for all voters (e.g., disabled voters, elderly people, and illiterate voters) [Al09a; OV04]. However, it has also been said that e-voting may bring about unintended effects by excluding large groups of citizens from participating in the democratic process, specifically those groups with less access to and familiarity with computers [OV09]. Another expectation held by many policy makers is that e-voting will increase overall voter turnout by providing a longer period to vote on Election Day [DP07]. However, researchers claim that extending the voting period does not necessarily increase voter turnout [Be03]. E-voting is also expected to increase overall voter turnout by increasing the motivation of people to vote, including youth voters [An09]. However, the capacity of e-voting technologies to increase the motivation of people to vote has been doubted by several researchers [DBoT11; OV09; Wi08]. Researchers argue that e-voting can encourage those voters who vote occasionally, but it does not increase the political participation of non-voters [MM06]. Instead, some researchers claim that e-voting (particularly I-voting) seems to increase inequalities in voting participation [BV10]. In conclusion, the assumptions that e-voting systems will improve the level of voter turnout have either been proved to be incorrect or have hardly been tested empirically. Some researchers found that while e-voting may indeed increase voter turnout in the beginning, it will either decrease or go back to the original level as soon as people get used to the technology [Be03]. Finally, we are repeatedly reminded that voter turnout may be quickly reduced by organizational and technical constraints [Be03].

Researchers claim that e-voting may foster greater political participation through increased transparency of the electoral process, improved accessibility for all voters, as well as increased voter turnout [KR10]. The issue of whether e-voting can indeed empower citizens has been questioned because e-voting removes the current public control inscribed in the traditional voting process, even though voters can both verify whether their ballot has been taken into account and participate in controlling the electoral process [Be07]. However, although some algorithms do provide voters with a way to check if their votes have been taken into account, they "can neither access the code, nor see the type of algorithm used, nor check that the machine is well configured and that the administration or other third parties do not manipulate voters" [Be07, pp. 32-33].

A very important argument behind e-voting technologies is the expectation of improved accuracy and elimination of spoiled votes [DP07] as well as increased efficiency and reduced waiting time. This solves the problem of finding volunteers and election officials [DP07]. Furthermore, with e-voting, election results could theoretically be determined a few minutes after the poll stations have closed [An09]. Increased efficiency is viewed as crucial for dealing with the current high costs related to elections [DP07]. The ability of e-voting to reduce costs has, however, been dismissed or doubted in various reports due to lack of strong empirical evidence [DBoT11]. Furthermore, when considering the rewards offered by the different e-voting technologies (e.g., in term of convenience and efficiency), it is questionable whether these are worth the additional

security risks (e.g., fraud, loss of citizens' confidence) imposed on our democracy [Be07].

3 Highlights from the Literature

Literature within the field of e-voting has been growing rapidly. E-voting constitutes a relatively young field of research where a large part of the studies originated in the U.S. [Ba06], although the number of European studies is increasing. These studies vary in many different ways. Some of the studies are about e-voting in supervised environments, while others are about I-voting over the Internet. Some studies report experimentations, while others are about real elections. Finally, the studies have often conducted in different contexts [Be03] with different samples of the population. Furthermore, while there has initially been a strong focus on technical dimensions related to the introduction of e-voting technologies [Be03], we now find a number of studies that focus on non-technical dimensions (i.e., socio-cultural, organizational, and political dimensions). The literature that focuses on non-technical dimensions comes from a wide variety of fields and disciplines (e.g., sociology, political science, communication, and Information Systems), drawing upon different theories and methods [Ba06]. This literature can be broadly divided into two domains: one that addresses issues related to the medium, the actual e-voting technology, and one that moves beyond the medium to address different issues, including organizational and legal aspects, the individual voters, traditions and rituals, etc. I will now provide highlights from these two domains, but will focus predominantly on the latter.

3.1 The Medium: E-voting Technologies

One of the main issues with e-voting technologies is that they challenge the basic fundamental principles necessary for democratic elections, for example, the principle of public control. Voting and tallying processes, which are currently under public control, become "black-boxed" behind computers, providing the public with limited access. This implies, among other things, that it is difficult for the public to detect failures and/or tampering incidents [Ba10; GH07; Lo08]. The principle of anonymity and secrecy of voters has continuously been threatened, especially by I-voting, which has not been able to provide a way to verify that the cast ballot indeed belongs to the correct voter. Thus, we can neither be sure that votes will remain secret, nor can we prevent vote buying or family voting (with I-voting) [Be07]. It has been said that the secret ballot "is the jewel in the democratic crown" [BP90, p. 311], providing an indispensable value which must not be compromised.

Security is one of the main evaluation criteria and topics discussed across the literature. This refers to the technical security of the actual technology (e.g., cryptographic verification and mathematical calculations to ensure voter verifiability, ballot box accuracy, etc.), but it also refers to issues related to voters (e.g., eligibility, privacy protection, anonymity, and secrecy of voters) [Be03; PM07]. Usability is another central topic that has been discussed since e-voting's earliest stages. Usability refers to

preventing voting errors, the system's ease of use, as well as accessibility [PM07]. These studies investigate interface design and the implications of graphical elements on usability and accessibility for voters [SLL09]. Some of the findings conclude that basic universal usability concepts and plain language address many of the problematic issues. For instance, the chronological order of candidates may influence people's voting [SLL09]. Finally, some researchers investigate ways in which ballot graphics can help voters with cognitive disabilities (e.g., verbal comprehension, reading ability, etc.) [SLL09].

If we look at the traditional paper-based system, most of the processes are in fact behind the stage and hidden from most voters. The practices of casting a ballot form a well-oiled "machine" and fades into the background: "its efficiency and its acceptance by the citizenry is signified by its *disappearance* in the sense that it becomes a *routine* taken for granted and not an 'issue'" [Ca06, p. 194]. Thus, it is this invisibility that, to some degree, allows the system to work smoothly. A similar argument has been made about e-voting technologies and about how important it is that these are 'invisible' to users [Be03].

3.2 Beyond the Medium: Socio-cultural, Political and Organizational Changes

Although most projects focus predominantly on technical aspects, recently there have been more studies that focus on social, organizational, political, and legal issues [Be03; WVM07; XM04]. It has been said that although technical dimensions are indeed important, "*trust* in the *system* seems to be more important than the technical characteristics themselves" [Be03, pp. 725-726, emphasis added]. However, what does *trust* mean in this context, and what does *the system* refer to?

The concepts of trust, reliability, and confidence are central to e-voting literature. However, their definition and usage vary across the articles and the disciplines. For example, Besselaar et al. [Be03] use the concepts trust and reliability interchangeably to refer to two domains: trust in the technology (in terms of safety, internal fraud, external hackers, etc.) and trust in the electoral process (e.g., protection of anonymity and secrecy of all the votes). However, many of the existing definitions focus on just one of these domains. For example, the concepts of trust and confidence have been defined as the confidence that the election process produces fair outcomes and that the ballot was counted accurately [AHL08; HMP09] a viewpoint mainly concerned about trust in the electoral process. Taking into account the different definitions of trust, these can be divided into two main categories: trust in technology [Be03; Ru05] and trust in the very mechanisms of our democracy, i.e., the actual electoral machinery and the process that records and counts votes [AHL08; HMP09; Ru05].

3.2.1 Voters' Trust in the Technology

Many studies investigate the effects of socio-demographic, geographic, and technical factors on voters' evaluation of the different e-voting technologies [Al09a]. They investigate how the voters' trust in e-voting technologies is influenced by individual

variables. So far, the most common demographic variables are gender, age, income, and education. There are also different findings for each of these variables. For example, when it comes to gender, there are no straight answers: one study, which tested the same e-voting system across several countries in Europe in different settings, found that women tend to be more positive about the usability of e-voting systems [Be03]. However, many other studies do not find gender to be a significant factor affecting trust in e-voting [AKP11; MM06]. When it comes to age, according to several studies, young people are more interested in technology than in politics; elderly voters are less confident with e-voting but motivated to participate in elections [Ca06]. One study found that youth, to a greater extent than the elderly, were inclined to cast their ballot using e-voting [MM06]. However, a number of studies found that older voters tended to be more confident with e-voting even if they found it more difficult to use [AHL08]. This has been attributed to their greater familiarity with participation in electoral processes [AKP11]. Furthermore, several researchers found that younger voters are more likely to be critical of e-voting because they are equipped with better computer skills and are more aware than their older counterparts of the vulnerability of technologies [AKP11; OV04]. One study found that the positive effect of education on voter confidence in e-voting is statistically significant [AHL08]. Another study found that highly-educated people tend to oppose e-voting technologies [SAH10], while yet another study found that education in itself has a limited direct impact on voters' trust in technology, as it is only those who have no or very little education who were significantly less in favour of e-voting [Ca06]. When education and profession are correlated with age, we find that educated people under the age of 50 are more in favour of e-voting [Ca06]. Finally, language can be significant in some contexts and countries. For example, in the parts of Estonia, where the population only speaks Russian and would, therefore, be unable to use an I-voting system implemented in Estonian [BV10].

A few studies have tested e-voting technologies across several countries. For example, Besselaar [Be03], who tested an e-voting application across four countries and five different settings, found that the rural community network in eastern Finland was more positive toward e-voting technologies than the Italian trade union. It is, however, difficult, if not impossible, to draw clear conclusions about different countries based on the various findings because the samples often tend to be either too small and/or too different; thus do not provide sufficient grounds for comparison. Some researchers agree that it is not easy to directly extrapolate such findings to other local contexts [AKP11].

We also find many studies that investigate the effects of different e-voting technologies on voters' confidence [Al09a; Be07; HMP09; SAH10]. The findings of these studies vary by country and the political context. For example, researchers found out that voters in Italy, France, and Finland tend to trust I-voting more [Be03]. There are, however, relatively consistent results across the studies (at least in the U.S.) when it comes to the impact that the voting medium has on voters' confidence. Voters often tend to have more confidence in paper ballots than in e-voting machines [AHL08; AS07; HL10; St09] and they, female voters especially, tend to view the paper ballot as the most anonymous way of voting [JHG08]. Furthermore, voters tend to have more confidence in optical scan when compared to e-voting machines [Ha09; St09]. However, recent studies conducted in the U.S. and in the Netherlands reveal that more voters expressed confidence in the

direct recording electronic (DRE) voting machines than in paper ballot voting [HL10; SAH10]. Finally, several researchers found that people tend to be more confident if they vote using the technology they like [SAH10]. Other attributes that have been correlated to people's confidence in e-voting are computer literacy, Internet use, and experience with equipment [Be03]. Several researchers claim that having a paper audit trail when deploying e-voting increases voters' confidence [Lo08], but there have been several studies recently that either point to a lack of empirical evidence [Ba06] or claim that there is no difference in voters' perceptions between voting machines with or without a paper trail [JHG08].

3.2.2 Voters' Trust in the Electoral Process: Individual and Universal Level

The second category of trust refers to the basic machinery of democracy—the actual mechanisms that record and count the votes. In reviewing the literature, public trust in the electoral machinery can be further divided into individual trust and universal trust. Individual trust implies confidence that every individual voter can verify that her ballot was counted accurately and as intended [AHL08; HMP09; So09]. While this focuses on the individual voter and her experiences, universal trust has a broader focus on the public and the general mechanisms for fulfilling the basic principles of democracy, for instance, public control, which implies that anyone has the possibility to witness, control, and/or scrutinize the correctness of the voting and tallying process [Ca06; So09]. The trust of the general public in the traditional procedure is influenced by the fact that the process is open to public control, and it is based on the simple mechanism of counting the paper ballots [Ca06].

There are various procedures for ensuring the principles of democracy and these are supported by complex chains of regulations. Elections are always carried out by different surveying authorities. For example, representatives of each political party, election officials, and volunteers are on-site, guaranteeing public control and overseeing the counting process. These procedures, which ensure the public nature of elections, are also supported by national laws that are rigorously enforced by different procedures (e.g., handling paper ballots, ballot boxes, voter identification, recount, etc. [DBoT11; So09; XM04]. Replacing paper ballots and pencil regulations implies that many of these regulations and laws will have to be reconfigured to accommodate the new technology [DBoT11; Lo08]. The principles of democracy are also enforced by the physical properties of the different materials. For example, the principles of anonymity and secrecy are enforced by the physical properties of the polling booth [XM04]. This will have to change when introducing e-voting [Ca06; XM04].

Although paper-voting systems have evolved throughout the years, they have always maintained a self-evident simplicity enabling everyone to easily understand the counting system without any special technical knowledge [Ru05; So09]. This will not be the case when deploying e-voting technologies, where IT knowledge is necessary [Ba10].

Recently, several researchers have investigated the relationship between voters' confidence in voting systems and other variables [GH09; St09]. Thus, the literature focusing on voters' attitudes, experiences, and expectations has increased rapidly [Ca06;

HV00; OV04; OV09]. Several researchers found that there are significant differences in voter confidence along both racial and partisan lines [HL10]. This seems to apply mostly to studies in the U.S. For example, Alvarez et al. [AHL08] found that African-Americans have less confidence in the electoral process than white people. Voter confidence can also be influenced by 'the winner effect,' which implies that voters for winning candidates tend to express greater confidence than those who voted for losing candidates [HL10; SAH10]. It has been noted that this phenomenon applies more to the American context, as political views were rather significant in the U.S.[St09], but that was not the case in Europe [HL10].

Voters' familiarity with the electoral process can also influence their view of e-voting [AHL08]. But this is related to a voter's experience at the polling place as well as their experience with election officials and poll workers. For example, voters' view of e-voting can be influenced by whether they experience having to wait in long lines [HMP09]. Little attention has been given to the role of the administration in the electoral process [Ha03; HMP09], even though poll workers have been described as "the Achilles' heel of the elections process" [HMP09, p. 508]. A number of studies have been investigating how voters' confidence is affected by their experiences at the polls and the experiences they have with poll workers [AHL08; Cl08; GH09; Ha09; HMP09, SAH10]. Voters' experiences with poll workers are important, as it is an integral component of the voting process [HMP09, 510]. A recent study shows that voters who rate their interaction with poll workers highly are more likely to be confident that their votes will be counted correctly [HMP09]. Another important variable that influences voter trust is the mode of voting [AAH07; Al09b; AS07; Ha09; St09]. Researchers found that voters who cast their ballot in-person on Election Day have significantly higher confidence than those who cast absentee ballots [HL10; SAH10; AHL08].

Several studies link voters' confidence to voters' general trust in government [AHL08]. For example, in a pilot study in Columbia, researchers found the percentage of respondents who claimed to trust e-voting was exceptionally high, and they point out that this probably relates to the relatively low level of public confidence in elections across several countries in Latin America [Al09a]. A couple of studies in the U.S. found that African-American voters tend to have less confidence in voting; researchers point out that this is most likely shaped by the historical discrimination that these voters experienced [Ha09; SAH10]. However, it has been argued that voters' trust in the government is not a sub-category of voter confidence and the two concepts are not necessarily the same [AHL08]. While voter confidence in the electoral process does not necessarily stem from a voter's general trust in government [HMP09], a general faith and trust in politicians appears to foster an acceptance of e-voting.

While the above research has focused on the interactions with election officials, other researchers argue, that voters' beliefs about and perceptions of privacy may be more critical. For example, Gerber et al. [Ge09] view the act of voting as an individual political behaviour that is influenced by voters' perception of ballot secrecy. They found out that there is a correlation between the belief that ballots are actually kept secret and race and education [Ge09].

A new article by Karpwotiz et al. [Ka11] focuses on voters' perceptions of privacy and its relationship to the political norms of the communities where voters live. The study shows how a community's political norms have great influence on voter behaviour. For example, voters who are told that the norm in the neighbourhood is to vote are more likely to vote. They conclude that concerns about privacy are prevalent among those who are against their community's political norm [Ka11].

The introduction of e-voting challenges conceptions of democracy, with its emphasis on efficiency, a trend that corresponds to new public management [Qi10]. The different forms of political participation and voting rituals anchored in political cultures are widely debated in some articles. These civic rituals and forms of political participation are manifested in different ways across the various cultures and countries. For instance, some countries in Europe (e.g., Switzerland) tend to value the opportunity given to citizens to be frequently consulted (e.g., through referendum) [Tr07]. Some scholars emphasize that the act of voting is more than simply indicating a political preference but rather a necessary public ritual that is part of a social solidarity binding citizens together [MG01]. Furthermore, concerns have been voiced about the impact that e-voting technologies may have on our governing and electoral procedures, which have been shaped by traditions, symbolic rituals, and material customs [Ca06]. Some researchers are concerned that these traditions may be lost or destroyed by e-voting technologies and that it may have a negative influence on the political culture [OV04]. This includes creating a larger gap between government and citizens and decreasing voter participation and turnout [OV04; OV09].

3.2.3 Influence of Other Relevant Stakeholders: Media, Politicians and Vendors

As can be seen above, several researchers have started to gradually move away from focusing solely on technology and have begun focusing on the voters and the role of administration and management. There are, however, other stakeholders who are equally important and powerful. One of the stakeholders with outsized influence is the media [R08]. A recent study shows how a communication campaign before the electronic voting stimulated citizens' curiosity and interest in elections [Ca06]. Furthermore, several studies have noted the importance of political support [Be03]. Similarly, Xenakis and Macintosh [XM04] describe how trust in the system of counting was developed through special reference to Commission's report regarding the Deputy Returning Officer and the acceptance that the project gained due to his good leadership.

One of the most dominant topics in the literature is the relatively strong influence privately-owned vendors have had thus far [Ru05]. In the U.S. most e-voting initiatives have been vendor-led. Therefore, several articles highlight the importance of moving away from vendor-led developments to initiatives led by scientists and/or another qualified, trusted third-party body to preserve public trust and ensure, among other things, that profit is not the dominant motive behind e-voting innovations. In an interesting article, Rubin [Ru05] refers to an editorial in the *New York Times* that draws similarities between election machines and gambling machines, as in both cases it is not easy for the user to verify the activity performed. However, while e-voting vendors claim their software is a trade secret, The Gaming Control Board has copies of every

piece of gambling device software currently being used. Rubin [Ru05] refers to Dark source—an artwork displaying the source code of a commercial electronic voting machine—to reflect upon our current state, in which the critical infrastructure of democracy is becoming privately owned. It has, therefore, been repeatedly argued in the literature that the software (e.g., algorithms and codes) running our democracy should be opened to public scrutiny [Be07; Ru05]. As Raymond says: "Given enough eyeballs, all bugs are shallow" [Ra00, p. 30]. Several articles have suggested different ways of dealing with the controversial topic of privately-owned vendors and the maintenance of public control. For example, several suggest having an independent, official authority, a qualified and trusted third-party, as well as legal regulations [DBoT11; So09] to formally certify the chosen solution [An09]. Some of the problems with the (re)certification process is that it takes such a long time that vendors are often too slow to fix their systems [Ba10]. Nevertheless, many researchers encourage the participation of all stakeholders, including policy-makers, technologists, and, most of all, citizens [Ca06; VSD11]. Finally, there are different incentives for outsourcing e-voting initiatives, some of which are aimed at reducing costs and improving efficiency. Oostveen [Oo10] who studied e-voting initiatives in the Netherlands (drawing upon action research) points to government agencies' lack of knowledge in identifying appropriate voting technologies, enforcing security requirements, and monitoring performances. She criticizes the Dutch government for losing the ownership over the election process to the private sector.

4 Discussion and Conclusion

So far, I have synthesized and mapped the different specific topics that are discussed across the research projects. I will now provide a typology, a broader, more general map classifying and clustering the different topics into themes. The three main interrelated themes that the different studies investigate are: political participation in general (e.g., voting behaviour and turnout), *trust* in e-voting technology, and *use* of e-voting technology. These studies investigate which factors have a significant impact on each of these themes and the extent of this impact. These factors can be grouped into five broad categories. The first category refers to the *voting method* (mode of voting) and the *medium* used to cast the ballot. This includes investigation of different modes of voting (e.g., voting at polling stations vs. remote voting), different media (e.g., absentee ballots, papers, DREs, I-voting); and different voting locations (e.g., home, workplace). The category of voting method also includes other variables, for example, design and usability of the system, the use of paper audit trail, as well as transparency of the code behind the software. The second category refers to the *voter*. This includes the voters' socio-demographic characteristics (gender, age, income, education, race, ethnic origin, and regional classification (urban vs. rural)), as well as their knowledge, expectations, and experience with computers. Another important factor is the voters' trust in government and politicians in general, and more specifically, their trust in the electoral process, including the fulfilment of the secrecy principle (i.e. privacy and anonymity of election decisions) and accountability (i.e. the ability to verify the vote). The voters' knowledge, expectations, and experience of the electoral process also have an influence, including their familiarity and previous experience of interactions with poll workers and

election officials. Finally, in some studies, voters' political preferences have also been included as a variable. The third category refers to civic *rituals, traditions, and norms* surrounding political participation and elections. Finally, the forth category refers to the *type of election* (e.g., national, European election, local election), and the fifth category refers to the influence of *other stakeholders*, including the media, vendors, and support of governmental institutions and/or political parties.

The different studies then investigate the influence of these categories and factors on political participation, as well as trust and use of e-voting. For example, a study typically investigates the influence the voting method, the characteristics of the voter, and the type of elections on political participation (e.g., in terms of voter turnout) has on the trust voters may express toward e-voting, and/or on use of e-voting technologies.

Many of the findings presented above are context-dependent, while others seem to be repeated across different contexts and can therefore be generalized to a certain extent. I will now use the typology presented above in order to provide a better overview of the findings that is generalizable - i.e., can travel beyond a specific setting. When it comes to the voting medium, one of the repeated findings is that technical and organizational issues (e.g., poor design and usability, installing hardware, software, registration) can reduce voter turnout [Be03]. The voters' level of trust and confidence changes depending upon the voting medium used and the specific setting (e.g., type of elections, country). However, one can detect general repeating patterns, whereby voters often tend to have more confidence in paper ballots than in e-voting technologies. Furthermore, the confidence of those who vote in-person seems to be relatively higher than those who vote remotely (e.g., absentee ballot, I-voting). When looking at the influence of the e-voting system on voter turnout, most studies seem to dismiss the correlation between the two. There is a correlation between voter turnout and the type of election, whereby turnout is consistently higher at national elections than at local elections. When it comes to the correlation between voter turnout and e-voting technology, the research findings are not completely consistent. Several studies claim that e-voting seems to have an impact on turnout; however, some claim that the impact is temporary and/or insignificant.

If we look at the voters and their impact on political participation, trust, and use of e-voting technologies, we can identify several interesting correlations. For instance, gender, age, and education seem to have some impact on voters' trust in e-voting. However the extent to which this impact is significant is rather unclear and cannot be generalized. One of the main findings that can be drawn in relation to age is that it influences the level of political participation. This finding refers to the general phenomenon of decline in younger voters [OV04]. Several studies confirm that there is a significant correlation between people's confidence in e-voting and computing literacy, Internet use, and experience with equipment. Furthermore, voter confidence in the electoral process, including expectations, familiarity, and experiences (e.g., interactions with poll workers) have some influence on their view of e-voting. Trust in the electoral process is related to the voters' general trust in government and politicians, but whether it is a positive or negative impact depends on the context. For example, Columbia reported high level of confidence in e-voting [Al09a], while African-Americans in the

U.S. reported less confidence in e-voting [SAH10]. It is clear that voters' trust in government and politicians have influence on their trust in e-voting; however, the degree of this influence varies across the particular countries and settings. These were the findings identified as generalizable; however, many of the different studies' findings are bound to their specific contexts. For example, the 'winner effect' as well as the differences in voter confidence along partisan and racial lines are phenomena that can so far only be applied to the U.S. One of the challenges with such findings is that it is often difficult to draw clear conclusions from the different findings, as these cannot be directly extrapolated to other contexts [AKP11].

There is a need for further studies that provide in-depth investigations of the non-technical aspects and the social impact of e-voting technologies. Most of the studies conducted so far draw upon quantitative methods (e.g. statistical analysis and surveys), with very few exceptions of studies that use ethnographies, case studies and other qualitative methods [e.g., Ba06; Ca06; MG01; OV04, OV09]. While quantitative studies are indeed valuable in explaining *what* happens when introducing e-voting technologies into a particular setting, they tend to come short in explaining *why* things happen. This leaves many questions unanswered. Why some variables are significantly relevant in particular contexts but not in others? For example, why do women tend to be more positive than men about the usability of e-voting systems [Be03]? Why are there differences between the attitudes of voters coming from diverse countries and different communities? For example, the differences identified by Besselaar [Be03] of a rural community network and a trade union from different countries.

In some studies, the researchers try to answer the question of *why* these things happen, but because their quantitative data does not enable them to form such conclusions, they end up proposing what they view as potential interpretations to the phenomenon. For example, it has been said that voters who cast their ballot in-person on Election Day have more confidence than those who cast absentee ballot [HL10; SAH10]. The authors propose a potential explanation that points to the fact that with absentee ballots, voters have to send their ballots through the postal service and can thereby not be sure whether their ballot was received in the time frame required for counting the ballots [HL10]. However, these are potential interpretations and explanations that are not directly based upon the empirical data collected. Similar examples can be found in studies [e.g., Al09a; SAH10] that try to explain a relatively surprising finding (e.g., high or low level of trust in e-voting) by referring to contextual or historical factors—variables and data that was not collected in the study (e.g., confidence in elections in general or to historical discrimination experienced by voters). In order to gain a more critical and in-depth understanding of such contextual and historical factors, there is a need for detailed qualitative studies into the various ways in which e-voting technologies change the way in which we practice democracy, focusing on election practices and the voters' political participation. Furthermore, there is a need for detailed qualitative studies of real-life experiments with e-voting technologies [e.g., OV09]. We know from the field of healthcare IT that studies of real-life experiments can inform discussions about design and implementations in a more critical and reflective way than those discussions that are grounded in real-life experiences and expectations.

Acknowledgement

The author was supported in part by grant 10-092309 from the Danish Council for Strategic Research, Program Commission on Strategic Growth Technologies. The author would also like to thank Kjetil Rødje for his careful feedback.

Bibliography

[AHL08] Alvarez, R. M., T. E. Hall, M. Llewellyn. 2008. Are Americans confident their ballots are counted? *Journal of Politics* 70: 754–766.

[AKP11] Alvarez, R. M., G. Katz, and J. Pomares. 2011. The Impact of new Technologies on Voter Confidence in Latin America: Evidence from E-Voting Experiments in Argentina and Columbia. *Journal of Information Technology & Politics* 8: 199-217.

[Al09a] Alvarez R. M. et. al. 2009. Assessing Voters' Attitudes towards Electronic Voting in Latin America: Evidence from Colombia's 2007 E-Voting Pilot. In *VOTE-ID 2009, LNCS 5767*, ed. P. Y. Ryan and B. Schoenmakers. 75–91. Springer: Berlin

[Al09b] Alvarez, R. M. et al. 2009. *2008 survey of the performance of American elections.* Boston/Pasadena: Caltech/MIT Voting Technology Project.

[An09] Ansper A. et. al. 2009. Security and Trust for the Norwegian E-voting Pilot Project E-valg 2011. In *4th Nordic Conference on Secure IT Systems, NordSec 2009, 5838*, ed. Audun J¸Sang, T. Maseng and S. J. Knapskog, 207--222, Oslo: Springer.

[AS07] Atkeson, L. R. and K. L. Saunders. 2007. The Effect of Election Administration on Voter confidence: A local matter? *PS: Political Science and Politics* 40: 655-660.

[Ba06] Ballas, A. 2006. E-Voting: The Security Perspective, London School of Economics, 33.

[Ba10] Balzarotti D. et. al. 2010. An Experience in Testing the Security of Real-World Electronic Voting Systems. *IEEE Transactions on Software Engineering* 36: 453-473.

[Be03] Besselaar, V. D. et. al. 2003. Experiments with E-Voting Technology: Experiences and Lessons. *Building the Knowledge Economy: Issues, Applications, Case Studies*, P. Cunningham et al., ed. IOS Press.

[Be07] Benoist, E. et. al. 2007. Internet-Voting: opportunity or Threat for Democracy?.*VOTE-ID 2007, LNCS 4896*, ed. A. Alkassar and M. Volkamer R. 29-37. Springer: Berlin.

[BP90] Brennan G. and P. Pettit. 1990. Unveiling the Vote. *British Journal of Political Science* 20: 311-33.

[Ca06] Caporusso, L,et. al. 2006. Transition to Electronic Voting and Citizen Participation. In *Electronic voting 2006, GI lecture notes in informatics,* ed. R. Krimmer. 191-200. Bonn: GI.

[Cl08] Claassen, R. et. al. 2008. "At your service": Voter evaluations of poll worker performance. *American Politics Research* 36: 612–34.

[DBoT11] Danish Board of Technology, 2011. *E-valg- et valg for fremtiden?* Anbefalinger fra en arbeidsgruppe under Teknologirådet, Danish Board of Technology, Copenhagen.

[DP07] De C. D. and B. Preneel. 2007. Electronic Voting in Belgium: Past and Future. In *VOTE-ID 2007, LNCS 4896*, ed. A. Alkassar and M. Volkamer R. 76-87. Springer: Berlin.

[Ge09] Gerber A. et. al. 2009. Is There a Secret Ballot? Ballot Secrecy Perceptions and their Implications for Voting Behavior. Paper presented at the annual meeting of the *American Political Science Association*, Toronto, Canada, September 3-9, 2009.

[GH07] Gonggrijp, R., and W. Hengeveld. 2007. "Studying the Nedap/Groenendaal ES3B Voting Computer: A Computer Security Perspective." Proceedings of the Usenix/Accurate Electronic Voting Technology on Usenix/Accurate Electronic Voting Technology Workshop (Boston, MA). USENIX Association, Berkeley, CA.

[GH09] Gronke, P. And J. Hicks. 2009. Re-Examining voter confiedence as a metric for election performance. Paper presented at the annual meeting of the *Midwest Political ScIene Assosciation,* Chicago, IL: April 2-5, 2009

[Ha03] Hall, T. E. 2003. Public participation in election management: The case of language minority voters. *American Review of Public Administration* 33:407–22

[Ha09] Hall, T. E. 2009. Voter attitudes toward poll workers in the 2008 election. Paper presented at the annual meeting of the *Midwest Political ScIene Assosciation,* Chicago, IL: April 2-5, 2009

[HL10] Hall T. and L. Loeber. 2010. Electronic Elections in a Politicized Polity. In *Electronic Voting 2010, GI lecture notes in informatics,* ed. R. Krimmer & R. Grimm. 193-212. Bonn: GI.

[HMP09] Hall T. E., J. Q. Monson, K. D. Patterson. 2009. The Human Dimension of Elections: How Poll Workers Shape Public Confidence in Elections. *Political Research Quarterly* 62: 507-522

[HV00] Hacker, K. & Van Dijk, Jan (ed.) 2000, *Digital Democracy, Issues of Theory and Practice.* London: Sage.

[JHG08] Jong, M. de; van J. Hoof, J. Gosselt. 2008. Voters' Perceptions of Voting Technology: Paper Ballots Versus Voting Machine With and Without Paper Audit Trail. *Social Science Computer Review* 26: 339-410.

[Ka11] Karpwotiz, C. F et. al. 2011. Political Norms and the Private Act of Voting. *Public Opinion Quarterly* 75: 659-685

[KR10] R. Krimmer and R. Grimm (Eds.), 2010. *Electronic Voting 2010, GI lecture notes in informatics*. Bonn: GI.

[Lo08] Loeber, L. 2008. E-voting in the Netherlands: From General Acceptance to General Doubt in Two Years. In *Electronic Voting 2008, GI Lecture Notes in Informatics,* ed. R. Krimmer, and R. Grimm. 21–30. Bonn: GI.

[MG01] Mohen, J. and J. Glidden. 2001. The Case for Internet Voting. *Communications of the ACM* 44: 72-85.

[MM06] Madise Ü. and T. Martens. 2006. E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In *Electronic Voting 2006, GI Lecture Notes in Informatics,* ed. R. Krimmer. 15–26. Bonn: GI

[Oo10] Oostveen, A.-M. 2010. Outsourcing Democracy: Losing Control of E-voting in the Netherlands. *Policy & Internet*. 2. Article 8.

[OV04] Oostveen, A.-M. and P. Van den Besselaar. 2004. Internet voting technologies and civic participation, the users perspective. *Javnost / The Public.* XI, 61-78.

[OV09] Oostveen, A.-M. and P. Van den Besselaar, 2009. Users' experiences with e-voting: A comparative case study. *International Journal of Electronic Governance* 2: 357-377.

[PM07] Puiggali J. and V. Morales-Rocha. 2007. Remote Voting Schemes: A Comparative Analysis. In *Vote-ID 2007, LNCS 4896,* ed. A. Alkassar and M. Volkamer 29-37. Springer: Berlin.

[Qi10] Qian, H. 2010. Global perspectives on e-governance: from government-driven to citizen-centric public service delivery. In *International Conference on Theory and Practice of Electronic Governance*, ed. Jim D. and T. Janowski. 1-8. ACM: New York, USA.

[Ra00] Raymond, E. S. 2000. *The Cathedral and the Bazaar,* O'Reilly.

[Ru05] Rubin, B. 2005. Dark Source: Public Trust and the Secret at the Heart of the New Voting Machines. In Making Things Public. Atmosphere of Democracy. Latour

[SAH10] Stewart C. III, R. M. Alvarez, T. E. Hall. 2010. Voting Technology and the Election Experience: The 2009 Gubernatorial Races in New Jersey and Virginia. In *Electronic Voting 2010, GI Lecture Notes in Informatics,* ed. R. Krimmer & R. Grimm. 19–32. Bonn: GI

[So09] Schmidt, A. et. al. 2009. Developing a Legal Framework for Remote Electronic Voting. In *VOTE-ID 2009, LNCS 5767*, ed. P. Y. Ryan and B. Schoenmakers. 92-105. Springer: Berlin

[SLL09] Smith B., Laskowski S., and Lowry S. (2009). Implications of Graphics on Usability and Accessibility for the Voter. In *VOTE-ID 2009, LNCS 5767*, ed. P. Y. Ryan and B. Schoenmakers. 75–91. Springer: Berlin

[St09] Stewart III, C. 2009. Election technology and the voting experience in 2008. Paper presented at the annual meeting of the *Midwest Political science Association*, Chicago, IL: April 2-5, 2009.

[Tr07] Trechsel, A. H. 2007. Inclusiveness of Old and New Forms of Citizens' electoral Participation, Representation, 43: 111-121

[Wi08] Wilks-Heeg, S. 2008. Purity of Elections in the UK. Causes for Concern. Report by the Joseph Rowntree Reform Trust Ltd. Doubting the e-voting would increase voter turnout.

[WVM07] Weldemariam K., A. Vilafiorita, A. Mattioli. 2007. Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach. In *Vote-ID 2007, LNCS 4896,* ed. A. Alkassar and M. Volkamer 38-49. Springer: Berlin.

[VSD11] Volkamer,M.,O. Spycher. E. Dubuis, 2011. Measures to establish trust in Internet voting. In *International Conference on Theory and Practice of Electronic Governance*, ACM: New York, USA.

[XM04] Xenakis, A. and A. Macintosh. 2004. Major Issues in Electronic Voting in the context of the UK pilots. *Journal of E-Government* 1: 53-74.

Interpreting Babel: Classifying Electronic Voting Systems

Joshua Franklin, Jessica C. Myers

Election Assistance Commission
Washington D.C., United States of America
josh.michael.franklin@gmail.com, jescurmy@gmail.com

Abstract: In an effort to promote a greater understanding of the voting systems that sit in the middle of the election technology spectrum - somewhere between hand-counted paper ballots and Internet voting - this work presents a classification of the electronic voting technologies currently used in the United States. A classification structure is presented, and characteristics of current and future technologies are discussed. Finally, the paper concludes with a discussion on practically using the structure and future expansion to include other voting technologies.

1 Introduction

Electronic voting systems have been in use since the advent of optical scan and punch card technology [Jo03]. Since that time, new classes of voting equipment emerged, coinciding with the creation and development of the personal computer. In the United States, lever machines were introduced to modernize elections in the late 1800s [Ca01]. Over the next century, voting technology used in the U.S. changed dramatically. From touch screen machines to Internet voting, the voting landscape across the U.S. is now a tapestry of new technologies and aging equipment. As technology advances, more pressure is applied to election officials to expand their knowledge regarding voting system technology innovations and implementations.

Election administration in the U.S. is complex and necessitates the involvement and combined knowledge of federal, state, and local officials. Election administration and voting system implementation in the U.S. are decentralized, meaning the role and influence of federal and/or state government varies from jurisdiction to jurisdiction. In contrast, a number of other countries use a singular voting system with one version of hardware and software in one approved configuration. In those countries, one voting system is used everywhere and is centrally administered, with higher levels of government (i.e., national government) playing a more active role in elections. The lack of a singular, uniform voting system in the U.S. and decentralized election administration contributes to the diversity of voting system technology used in each election jurisdiction.

For example, *Figure 1*[1] is a map of Pennsylvania; each color represents a different voting system and each county is colored to represent the voting system used in that jurisdiction. Since there are so many manufacturers and systems in one state, it is unlikely that federal and state election officials could implement practices that would apply to all jurisdictions. This situation is not unique to Pennsylvania.

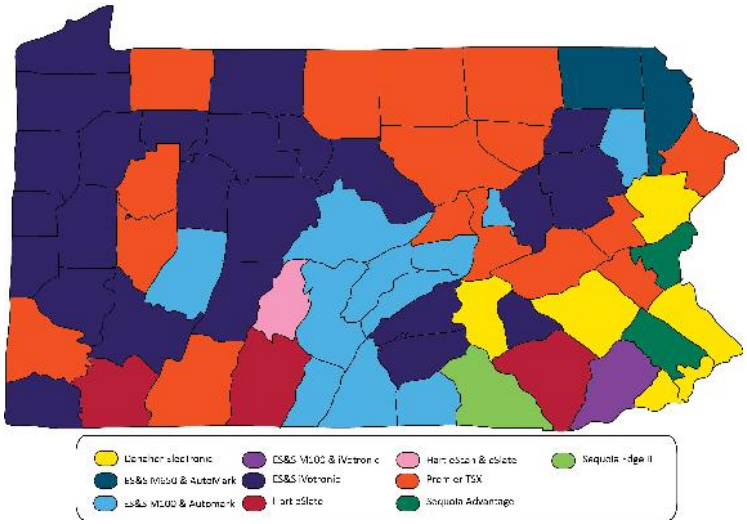


Fig. 1: Voting systems in Pennsylvania, 2008

Just as election administration practices differ, the types of voting technology used from country to country vary widely. Many countries use voter-marked, hand-counted paper ballots as a primary method of voting. Some of these countries are now exploring the newest voting technologies, including Internet voting. The massive leap from hand counted paper ballots to Internet voting skips over the middle ground of systems most commonly used in the United States: direct record electronic (DRE) and optical scan (OS) technologies. In an effort to promote a greater understanding of the voting systems that sit in the middle of the election technology spectrum - somewhere between hand counted paper ballots and Internet voting - this work presents a classification of the electronic voting technologies currently in use or available in the marketplace today.

In 2011, we developed a classification structure for Internet-voting systems during the course of researching and writing the U.S. Election Assistance Commission's *Survey of Internet Voting*. We discovered there is nothing clearly describing and classifying the equipment used in the U.S. This made it difficult for us to have a base of understanding and to convey certain concepts when talking with other countries about their process compared to the U.S. process. This led to a decision that we should create a classification structure for the systems used in the U.S. and then, eventually, create an overall structure combining all of the voting equipment available.

[1] Image based on a map from Pennsylvania Department of State, Secretary of the Commonwealth's Office, 2010.

The structure contained within the *Survey of Internet Voting* and the information contained in this paper derives from our combined experience as election officials at the state and federal level, as well as experience with election administration and election support at the local level. It is a difficult task to locate individuals who have experience with these systems at both the state and federal level, which we believe provides us with valuable insight into how to develop something useful for all stakeholders (i.e., federal certification programs, state certification programs and election officials, etc.) as well as familiarity with all of the systems discussed in this paper.

First, we developed a classification structure for electronic voting systems (not including remote electronic voting). Non-electronic voting systems (i.e., lever machines or hand-marked paper ballots) and punch-card voting systems are not included in this structure. Electronic voting systems used directly by voters are the primary focus of this discussion. Election management systems, which are composed of voting software and utilized on dedicated PCs for a variety of election related functions (e.g. ballot creation, ballot design, election definition, etc.), and voter registration systems are not discussed within this work. Hybrid voting systems, which are systems composed of multiple electronic voting categories, are discussed. Finally, the paper concludes with a discussion about the benefits of using the classification structure and the need to expand the classification structure to include remote electronic voting and future innovations.

2 Electronic Voting Classification Structure

The Electronic Voting Classification Structure (EVCS) is composed of four tiers: core technology, component, voter interface, and ballot presentation. *Figure 2* presents the classification structure developed to assist in the identification and classification of electronic voting systems.

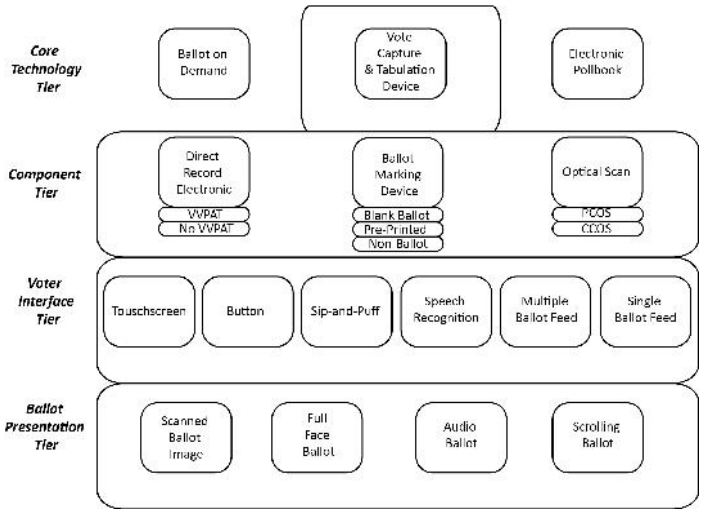


Fig. 2: Electronic Voting Classification Structure

Each tier denotes a specific characteristic, which allows for further classification of the voting system. Existing electronic voting systems can be distilled into functions and components based on the characteristics of these tiers, which fully describe a voting system. For instance, this structure can easily be used to classify a touch screen electronic voting system:

Core Technology => Vote Capture and Tabulation Device
Component => Direct Record Electronic
Voter Interface => Touch screen
Ballot Presentation => Scrolling Ballot

The process above classifies voting systems based on a set of pre-defined characteristics. The system qualifies as a vote capture and tabulation device because it captures and tabulates voter selections and does not print paper ballots or interface with a voter registration database. The hypothetical machine described above stores voter selections in an electronic format and is classified as a DRE system. In its most basic form, this structure can describe a voting system with four specific features, with each major feature corresponding to a tier. Detailed descriptions of the characteristics, properties, and items identified in each tier are provided in each section of this paper. Hybrid voting systems, consisting of more than one category in a tier, are becoming increasingly prevalent in the U.S. and are detailed in a later section of this paper. Many of the voting systems classified in this paper include a link in the citation to a video and/or images of how each system works.

2.1 Core Technology Tier

The core technology tier is the broadest classification of electronic voting technologies. Core Technology is defined by the overall function, goal, or purpose of the system, and has three categories:

- Vote Capture and Tabulation Device
- Ballot on Demand System
- Electronic Poll Book

The vote capture and tabulation device is the category in the structure covering the largest proportion of voting systems currently available and is the central focus of this work. Vote capture and tabulation device is the only core technology category directly interacting with voters; ballot on demand systems and electronic poll books are normally run and operated by election workers. Specifically, these devices accept voter input, record the input as voter selections, and tabulate these selections to provide election results.

In the U.S., ballot on demand systems are frequently implemented as an additional feature of a voting system. Usually they are combined with a vote capture and tabulation device, although they can function independently. Generally, they are not included within U.S. state or federal certification because they do not usually qualify as part of the voting system used for vote capture and tabulation. Many states print a large number of ballots in preparation for Election Day. The number of ballots printed is usually based on

a percentage of the total population of a county or municipality. Often, a large percentage of the pre-printed ballots are wasted because election officials must estimate turnout prior to Election Day. Ballot on demand systems print blank ballots as needed, which potentially allows jurisdictions to save some of the cost of printing ballots. Voters do not interact with or make selections with pure ballot on demand systems, as the systems only print blank ballots on blank paper stock as needed. An example of a ballot on demand system is the Advanced Ballot Solutions system recently reviewed in New Mexico [Nm11].

Electronic poll books are the third and final category of core technologies. Electronic poll books are used to interface with the list of registered voters. They denote whether a voter is registered properly and can create tokens (e.g., smartcards) to allow a voter access to a DRE component. Electronic poll books are usually comprised of software on laptops or tablet devices and utilize commercial or custom hardware and connect to the voter registration database via the cellular network or other network medium. An example of an electronic poll book is the Premiere Express Poll 4000 used in Georgia [Ke12].

2.2 Component Tier

There are three categories within the component tier with each category containing the following subcategories:

- Direct Record Electronic
    - With VVPAT
    - Without VVPAT
- Optical Scan
    - Precinct Count Optical Scan
    - Central Count Optical Scan
- Ballot Marking Device
    - Blank Stock
    - Pre-Printed Ballot
    - Non-Ballot

Equipment in the component tier is defined by where and how a voter's selections are stored. These selections can be stored on physical media (e.g., paper ballots) or electronic media (e.g., USB). In some cases this means a full ballot printout or receipt is provided for the voter to read and retain. In other cases voter selections are stored on paper but are not presented in a human readable format. These formats include encrypted voter selections, barcodes, or quick response (QR) codes, which require additional equipment, such as a barcode scanner in order to allow voters to review their selections.
DREs are commonly referred to as touch screens, although not all DREs are touch screens. DRE voting systems are not defined by their method of interface but rather by their method of storing voter selections. Due to this fact, it is possible to have a DRE voting system comprised solely of a commercial, off-the-shelf (COTS) personal computer with a keyboard and mouse. Some DREs use a voter verified paper audit trail (VVPAT), which stores voter selections on paper via an internal or external printer. With a VVPAT, voter selections are stored concurrently on physical and electronic media.

Some US states and election jurisdictions define physical storage (i.e., paper ballot) as the "ballot of record" and not the information stored electronically by the DRE. "Ballot of record" refers to the ballot, which will be used for official canvassing, vote tabulation, recounting, and record retention.

As stated previously, optical scan machines accept, read, record, store, and tabulate paper ballots. Optical scan machines fall into two subcategories: precinct count optical scan (PCOS) and central count optical scan (CCOS). The Hart eScan [Ha12] and ES&S M650 [El12] are examples of PCOS and CCOS systems respectively. Although this classification system does not make the distinction, optical scan equipment can be classified by the types of technology employed to digitally scan ballots (e.g., infrared, fax-bar, image scanning) [Jo03]. The voter interacts with PCOS components directly by individually scanning their ballot after making ballot selections. CCOS systems are used by an election jurisdiction to quickly tabulate large batches of ballots, so a voter is never afforded an opportunity to interact with the system. Most commonly, CCOS systems are used for absentee, military, overseas voters, and jurisdictions using a vote by mail system (e.g., Oregon). It is interesting to note that, at times, election staff may use PCOS as CCOS machines.

The ballot marking device component marks paper ballots with voter selections. This is accomplished via a touch screen or button interface, which is discussed in the next section. Voter selections are stored on paper but are entered and marked with an interface typically associated with a DRE. This feature is what distinguishes BMDs from optical scan and DREs. ES&S's AutoMark is employed by many election jurisdictions throughout the U.S. and is the most popular example of a BMD [Ci12]. AutoMark is but one type of BMD, and we identify three subcategories categories:

- Printing voter selections and a ballot in one operation onto blank paper stock;
- Printing voter selections onto a pre-printed ballot; and
- Printing voter selections onto a non-ballot format.

There are many ways voter selections can be printed into a non-ballot format. One possibility is printing voter selections onto a piece of paper smaller than the average ballot size and listing only the candidates the voter selected.

2.3 Interface Tier

The interface is the method in which a voter makes selections and interacts with a voting system. Frequently, voting systems have multiple interfaces to meet the accessibility requirements and needs of voter's with disabilities. An extreme example of a component with multiple interfaces is a DRE with a touch screen, button, sip-and-puff, and speech recognition capabilities. There are six categories in the interface tier:

- Multiple Ballot Feed
- Touch screen
- Button
- Single Ballot Feed
- Sip-and-Puff
- Speech Recognition

The single ballot feed interface is only associated with OS and ballot-marking device components and applies to scenarios where the voter feeds a single ballot into a voting system.

The multiple ballot feed interface category is associated with OS components. It does not typically include ballot-marking devices, except when the voting system is a hybrid, which is discussed later in this paper. Multiple ballot feed refers to situations in which many ballots from different voters are stacked in batches and fed into a CCOS component. Multiple ballot feed systems are most commonly used for military and overseas voters but may be used to double check or recount vote totals provided from multiple PCOS systems.

The touch screen, button, speech recognition, sip-and-puff, and mouse interfaces are all possible interfaces on BMD and DRE components. Touch screen interfaces are most commonly associated with DRE and BMD components. Button interfaces are provided on certain DREs, including the Danaher ELECTronic 1242 used in Delaware [De12] and the Virgin Islands [Vi12]. A button interface describes any voting system with buttons provided for the voter to interact with a component. These buttons may be built into the component's chassis or a tangible COTS keyboard. An example of a system with a keyboard interface is the Scytl/Hart Electronic Poll Book used in Washington, D.C. [Ha10]

Speech recognition and sip-and-puff interfaces are usually designed as options for persons with cognitive and/or physical disabilities. To our knowledge, speech recognition has not yet been commercially produced in an electronic voting system, although one prototype voting system using a speech recognition interface exists, the Prime III. Sip-and-puff is a binary input device, commonly used by voters with upper body paralysis [Cl12]. The sip-and-puff device is owned by the voter and is a "wand" or straw which allows the voter to inhale (sip) or exhale (puff) to navigate around the ballot, make ballot selections, and cast the ballot.

2.4 Presentation Tier

The presentation tier describes how ballots and, therefore, candidates, contests, and referendum/questions, are presented to voters. This is usually done in one of four ways:

- Full-Face Ballot
- Scrolling Ballot
- Scanned-Ballot Image
- Audio Ballot

If a voter's ballot is presented in its entirety, the system presents what is known as a full-face ballot. If the entire ballot is not presented upfront and the voter must scroll or navigate through the ballot to view it, it is called a scrolling ballot. Each state and jurisdiction has requirements regarding ballot presentation. For example, New York requires the ballot to be presented as a full-face ballot, resulting in a 21" ballot for their election in 2010.

The scanned-ballot image category describes a system that scans a ballot and presents this scanned image to the voter. The Dominion Imagecast presents the voter with a scanned-ballot image after the voter confirms their selections [Ne12]. Scanned-ballot images are often championed for their value to voters with disabilities, because all ballots are interpreted and tabulated the same way, no matter the interface used to input the data. More specifically, one method is used to gather voter selections from disabled voters and non-disabled voters. The system then uses the same data to tabulate results and requires no additional interaction from the voter allowing voters with dexterity problems to cast ballots in the same manner. Audio ballots are often used to meet accessibility requirements for U.S. voting systems and allow the voter to listen to an audio file, which reads the ballot to them.

3 Hybrid Voting Systems

Hybrid voting systems are voting systems that combine the functions and capabilities from several categories of the core technology and component tiers. Hybrid voting systems are the most recent additions to electronic voting technology and are in the process of being deployed in the U.S. As an example, a voting system might have the characteristics of both a BMD and DRE by combining both units into a single chassis and interface. A current example of this hybrid voting system is the Unisyn OVI [Un12].

Core Technology => Vote Capture and Tabulation Device
Component => DRE / Ballot-Marking Device
Voter Interface => Touch screen / Button / Sip–and–Puff
Ballot Presentation => Full -Face Ballot / Scrolling Ballot

Another example is the Dominion ImageCast used in New York [Ne12].
Core Technology => Vote Capture and Tabulation Device / Ballot on Demand
Component => Optical Scan / Direct Record Electronic / Ballot-Marking Device
Voter Interface => Single Ballot Feed / Touch Screen / Button / Sip–and–Puff
Ballot Presentation => Full-Face Ballot / Scrolling Ballot

In other cases, voting systems are combined in interesting ways. For example, stacking the ESS AutoMark on top of a precinct scanner, like ESS's M100 or DS200, is a fairly common set up in polling places across the U.S.

4 Applying the Classification Structure

The classification structure presented is useful in a number of ways. We believe a structure of this nature is necessary to develop and define a working language of electronic voting technologies. This is especially useful in the world of consumer electronics, which many of these voting technologies leverage, where systems are designed, developed, and depreciated within a few years. It often happens that voters, election administrators, election technologists, and other concerned parties are not speaking the same language when discussing voting technology. Through the publication of this information and the development of a classification structure, election officials can understand what characteristics different types of voting technology possess. Also, it can help those unfamiliar with certain types of systems to gain a foundation of understanding. Given enough time, iterative refinement, and acceptance, the structure can ensure that voting technology is described in a more succinct and meaningful manner. Common language and terminology may allow for better communication between election officials of different counties, states, or countries. Additionally, if those working with voting technology can understand each other and share information more easily, it is easier to share best practices and innovations, which promotes better elections.

This classification is useful for certification efforts in the United States as well as promoting a general understanding of the types of voting systems available. In the U.S., standards exist to test and certify voting equipment [Us12]. The classification system employed by this standard is based on a set of older standards that only envisioned DRE, optical scan, and punch card technology. These standards do not consider BMD technology or a number of interfaces described in this paper, such as keyboard input or speech recognition. By classifying systems with this structure, requirements can be tailored to test very specific functionality.

With a more detailed classification structure, election administrators can better understand what characteristics are needed to meet their jurisdiction's specific needs. Once these requirements are identified, it is easier to clearly specify and communicate those needs in a Request for Proposal (RFP) for procurement of a voting system. In the U.S., contracting for new voting technology is a high-risk process with long-term consequences. When purchasing new equipment, jurisdictions generally expect (and are usually told) new technology will last at least 10 years and will require maintenance contracts for upkeep and upgrades. The process of purchasing systems with the latest innovations must be balanced with the need to sustain aging technology for as long as possible. Legacy systems have technology that, at one time, was innovative and new but is now reaching the end of its life cycle. Many of the systems currently fielded across the U.S. qualify as legacy systems and will need to be replaced in the near future.

Figure 3 classifies the majority of electronic voting systems either in use or federally certified for use in the United States, including legacy systems and hybrid technologies. Only vote capture and tabulation devices are presented in this table.

Unit	***Core Technology***	***Component***	***Interface***	***Ballot Presentation***
AVS	VCTD	DRE	Touch screen / Button / Sip-and-Puff	Scrolling Ballot / Audio
Automark	VCTD	BMD	Touch screen / Button / Sip-and-Puff	Scrolling Ballot / Audio
Danaher ELECTronic	VCTD	DRE	Button / Sip-and-Puff	Full-Face Ballot / Audio
Diebold OS	VCTD	OS	Single Ballot Feed	Full-Face Ballot
Diebold TS	VCTD	DRE	Touch screen / Button / Sip-and-Puff	Scrolling Ballot / Audio
Dominion ImageCast (As used in New York)	VCTD/BOD	OS / DRE / BMD	Single Ballot Feed / Touch screen / Button / Sip-and-Puff	Full-Face Ballot / Scrolling Ballot / Audio
Dominion ICC	VCTD	OS	Multiple Ballot Feed	Full-Face Ballot
Dominion ICE	VCTD	OS / DRE / BMD	Single Ballot Feed / Touch screen / Button / Sip-and-Puff	Full-Face Ballot / Scrolling Ballot / Audio
Dominion ICP	VCTD	OS / DRE	Single Ballot Feed / Touch screen / Button / Sip-and-Puff	Full-Face Ballot / Audio
ES&S DS200	VCTD	OS	Single Ballot Feed	Full-Face Ballot
ES&S DS850	VCTD	OS	Multiple Ballot Feed	Full-Face Ballot
ES&S M100	VCTD	OS	Single Ballot Feed	Full-Face Ballot
ES&S M650	VCTD	OS	Multiple Ballot Feed	Full-Face Ballot
Hart eScan	VCTD	OS	Single Ballot Feed	Scrolling Ballot/Audio
Hart eSlate	VCTD	DRE	Button / Sip-and-Puff	Scrolling Ballot / Audio
Prime III	VCTD	DRE	Touch screen / Speech Recognition	Scrolling Ballot / Audio

Unit	***Core Technology***	***Component***	***Interface***	***Ballot Presentation***
Sequoia Advantage	VCTD	DRE	Button / Sip-and-Puff	Full-Face Ballot / Audio
Sequoia Edge	VCTD	DRE	Touch screen / Button / Sip-and-Puff	Scrolling Ballot / Audio
Sequoia Edge II	VCTD	DRE	Touch screen / Button / Sip-and-Puff	Scrolling Ballot / Audio
Unisyn OVCS	VCTD	OS	Multiple Ballot Feed	Full Face Ballot
Unisyn OVI	VCTD	DRE / BMD	Touch screen / Sip-and-Puff / Button	Full-Face Ballot / Scrolling Ballot / Audio
Unisyn OVO	VCTD	OS	Touch screen / Single Ballot Feed	Full-Face Ballot

Fig. 3: Classification of electronic voting systems in the US

Finally, this structure provides for possible combinations of voting technologies that may not exist or are in the design stages. An example of this could be:

Core Technology => Vote Capture and Tabulation Device / Electronic Poll Book
Component => Direct Record Electronic
Voter Interface => Touch Screen / Button / Sip-and-Puff
Ballot Presentation => Scrolling Ballot

This hypothetical system is a single machine that can access voter registration information as well as store voter selections. If a voter is identified on the voter roll and presented with the correct ballot all in one machine, this could save time at voter check-in and potentially cut election administration costs by requiring fewer poll workers and/or less redundant equipment. Additionally, looking at the classification structure could help spur the development and design of future voting technologies. The structure lays out the possible combinations in a simple and manageable format, which could help developers come up with new ways to combine different features in an effort to fully serve their customers' needs.

5 Conclusion

This paper creates standardized terms, as well as a classification structure, to provide election officials with a clearer picture of their own systems and to allow them to compare it with what is available. This structure is useful during the RFP process because election officials can clearly articulate their needs at the beginning of the process rather than sifting through all options and trying to decipher which system meets their needs. If election officials request to have voting system information presented to them using the Electronic Voting Classification Structure provided here, manufacturers can use this to describe systems in documentation and sales information, creating a level of standardization in terms and descriptions.

Additionally, in terms of information sharing, a common language and shared terminology is essential for promoting understanding. This common language is presented clearly and makes it easier for those trying to understand election administration practices (e.g., journalists and the media) to speak and write accurately about elections, which is of the utmost importance to election officials. This method breaks the system down into manageable pieces, making it easier to train poll workers and educate voters.

The only other methodology for classifying electronic voting systems, which the authors are aware of, was created by the United States National Institute of Standards and Technology (NIST). This structure is part of the Draft Voluntary Voting System Guidelines 2.0 and provides a voting system and device class structure [Te07]. The NIST structure is commendable in that it is detailed, unambiguous, and provides strict terminology for all parties involved in the U.S. voting system testing and certification process (e.g., voting system manufacturers, laboratories, and governmental organizations). The NIST structure creates a hierarchy that defines devices and assigns them a level within the hierarchy. An inheritance structure is formally provided. Additionally, a process for creating new voting system devices is provided for via the innovation class. We are concerned that the NIST structure may be too complicated and detailed for those outside of U.S. voting system certification, where a more practical and simplified structure is warranted. One of the primary reasons we provide the structure presented within this paper is to assist the stakeholders involved in day-to-day election administration with the knowledge and tools necessary to accurately and effectively conduct, monitor, maintain, and review elections. These stakeholders include contracting officers, election officials, members of the media, politicians, and the I.T. staff involved in maintaining election technology.

Future additions to this classification structure are vast and a multitude of possibilities exist. Practical first steps include classifying additional characteristics of the systems described in this paper (the four tiers) and creating distinct component tiers for ballot-on-demand systems and electronic poll books. New items could be added to the core functionality tier: card readers, ballot printers, barcode scanners, election management systems, token creators, and large ballot sorters. Additionally, the classification system could be extended to voting systems without hardware components, such as Internet voting systems. An Internet voting systems classification already exists and could be merged with this classification structure to provide a complete picture of voting systems [Us11]. U.S. election officials are already discussing voting systems that only use COTS

hardware components, such as iPads or desktop computers [Te11]. Other jurisdictions are even trying to crowdsource ideas to create next-generation voting systems [Lo10]. With all of these imaginative prospects on the horizon, surely the next-generation of electronic voting systems is closer than many believe. This is exciting for all parties within the election ecosystem-especially voters.

Bibliography

[Ca01] Caltech/MIT Voting Technology Project: Residual Votes Attributable to Technology: An Assessment of the Reliability of Existing Voting Equipment. Version 2, 2001. http://www.hss.caltech.edu/~voting/CalTech_MIT_Report_Version2.pdf

[Ci12] City of Detroit, Department of Elections: M100 and Automark Voting Systems. Accessed 2012. https://www.detroitmi.gov/DepartmentsandAgencies/DepartmentofElections/M100AutomarkVotingSystems.aspx

[Cl12] Clemson University, Human-Centered Computing Lab: Prime III. Accessed 2012. http://primevotingsystem.com/

[De12] Secretary of State, Delaware Board of Elections: Danaher Demonstration Video. Accessed 2012. http://elections.delaware.gov/services/voter/pdfs/psa.wmv

[El12] Election Systems & Software: Products and Services: Model 650™ Central Scanner. Accessed 2012. http://www.essvote.com/HTML/products/m650.html

[Ha10] Hart Intercivic: Washington, DC Awards Hart Electronic Poll book Contract. 2010. http://www.hartic.com/pr/99

[Ha12] Hart Intercivic: How to Vote Video. Accessed 2012. http://www.hartic.com/pages/114

[Jo03] Jones, D.: A Brief Illustrated History of Voting. University of Iowa, 2003. http://www.divms.uiowa.edu/~jones/voting/pictures/

[Ke12] Kennesaw State University, Center for Election Systems: Express Poll Images. Accessed 2012. http://elections.kennesaw.edu/?q=gallery/express-poll-images

[Lo10] Los Angeles County Registrar-Recorder/County Clerk: Public Information Hearing: The Future of Voting in California – "The People, The Equipment, The Costs." 2010. http://www.lavote.net/Voter/VSAP/PDFS/VSAP_Public_Info_Hearing-Future_of_Voting.pdf

[Ne12] New York State Board of Elections: Imagecast Demonstration video. Accessed 2012. http://www.vote-ny.com/english/machine-sequoia.php

[Nm11] Secretary of State, New Mexico; Summary Report: Voting System Certification – Independent Testing. 2011. http://www.sos.state.nm.us/pdf/SUMMARY-REPORT.pdf

[Te07] Technical Guidelines Development Committee: VVSG Recommendations to the EAC. 2007, page 89. http://www.eac.gov/assets/1/Page/TGDC%20Draft%20Guidelines.pdf

[Te11] Technical Guidelines Development Committee: Hardware Independent Voting Systems. 2011. www.nist.gov/itl/vote/upload/Presentation-HardwareIndependentVotingSystems.ppt

[Un12] Unisyn Voting Solutions: OpenElect Voting Interface (OVI). Accessed 2012. http://www.unisynvoting.com/products/ovi.htm

[Us11] U.S. Election Assistance Commission: A Survey of Internet Voting. 2011. http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

[Us12] U.S. Election Assistance Commission: 2005 Voluntary Voting System Guidelines. Accessed 2012. http://www.eac.gov/testing_and_certification/2005_vvsg.aspx

[Vi12] Virgin Islands Board of Elections: Equipment Demonstration. Accessed 2012. http://www.vivote.gov/content/election-equipment-demonstration

Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-Binding Elections and Approaches Proposed in Scientific Papers

Jurlind Budurushi, Stephan Neumann and Melanie Volkamer

Fachbereich Informatik – „SecUSo“
CASED / Technische Universität Darmstadt
Hochschulstraße 10
64289 Darmstadt, Germany
{name.surname}@cased.de

Abstract: Recently, the interest in electronic voting has increased as more and more states have started to implement such systems. At the same time, classical national ID cards are often being replaced by national electronic ID cards which enable citizens to securely identify and authenticate themselves over the Internet. Despite their popularity, the possibility of using eID cards for e-voting has not been adequately studied. This work surveys e-voting systems in which smart cards were used or were proposed to be used to support the voting process. We consider all types of smart cards, including those only for use in e-voting as well as existing and future national eID cards. In a two-step process, we will analyze the most interesting, real-world applications and proposals from a security, usability, and cost perspective, allowing us to derive our lessons learned. Upon these lessons, we show that the restricted-ID mechanism as implemented in the German eID card serves as an interesting basis for the integration of eID cards in e-voting. We outline that the risk of a “forced-abstention” attack can be mitigated by using the restricted-ID.

1 Introduction

Recently, the interest in electronic voting (e-voting) has increased, and many states are pushing for their use in legally binding elections. At the same time, states are adopting national eID cards, which provide a very secure way to identify and authenticate users over the Internet and thus allow citizens to interact with public authorities or private companies from their homes, even if they live abroad.

In e-voting, voter identification and authentication plays an important role in ensuring that only eligible voters may cast a vote, that those voters only cast a vote once, and that eligible voters are not prevented from voting. Therefore, using eIDs for voter identification and authentication in e-voting has a promising future in the field.
As smart cards like eIDs are no longer only used for the purpose of identification and authentication but also for storing sensitive information and securely processing some

parts of cryptographic protocols including signing and encrypting, these functionalities can also be used (and have also been used and proposed to be used) to increase the security of e-voting systems.

Since there are already real-world e-voting systems and approaches proposed in scientific papers which rely on or propose the usage of smart cards in different ways, the goal of this paper is to evaluate these systems and approaches in order to produce a list of lessons learned for future applications of existing eIDs as well as for future eIDs to better support existing and future electronic voting schemes.

Therefore, we will analyse the use of smart cards in the university elections in Austria, the national elections in Finland and Estonia, and the D21 election in Germany. Furthermore, we will evaluate scientific proposals including the application of the European Citizen Card, the German eID, and two scientific papers proposing additional functionalities for smart cards used in e-voting, namely the Votescript+ and Votinbox e-voting schemes.

Our lessons learned are manifold: Generally, legally binding elections should not use arbitrary smart cards but rather eID cards with which voters are familiar and which mitigate the risk of vote-selling significantly. In addition, we learned that there are no more secure alternatives to integrate current eIDs with very limited functionality (like the eID used in Austria and Estonia) as implemented in the corresponding systems. We concluded from the e-voting schemes Votescript+ and Votinbox that it is very important to find an adequate trade-off between necessary functionality, which increases the security of the overall e-voting system, and too much functionality, which increases the risk of vulnerabilities to the eID itself. We were able to point out that the idea presented in [BKG11] has the potential to improve the security of electronic voting in regards to coercion resistance. The Restricted-ID mechanism mitigates the risk of "forced-abstention" attacks against "less powerful" attackers, i.e., attackers who observe public channels and the Bulletin Board but are not able to break the used cryptographic protocols.

The remainder of the paper is structured as follows: section 2 gives a general overview of smart cards and a short list of smart card types we take into consideration. Section 3 describes real-world e-voting systems, defines appropriate evaluation criteria, and analyses these systems with respect to the proposed criteria. In section 4, we describe and analyse different scientific approaches that use smart cards that offer more functionality than the national eID cards, which have been used in current real-world e-voting systems. Section 5 summarizes the lessons learned and concludes with our contribution.

2 Smart Cards

According to [ISO7816] smart cards are plastic cards with embedded, integrated circuits and similar in size to today's payment cards. They can be used as an access-control device, making personal and business data available only to the appropriate users. Smart cards provide data portability and are designed from the ground up to be a secure system component [Ab02]. There are three different categories of smart cards according to [RE03]: integrated circuit (IC) memory cards, IC optical memory cards, and IC microprocessor cards. An IC memory card simply stores data in a secure manner. IC optical memory cards are the same as IC memory cards but have more memory capacity. An IC microprocessor card, on the other hand, can process, i.e., add, delete, or manipulate, information in the memory of the card, allowing for a variety of applications and dynamic read/write capabilities.

Smart cards are used in e-voting schemes to securely identify and authenticate voters as well as to secure the actual e-voting scheme including, signing and encrypting messages and/or votes. Usually e-voting schemes use IC microprocessor cards because they are based on cryptographic protocols and primitives. Thus, when we refer to smart cards in this paper, we are referring to IC microprocessor cards.

We consider different types of smart cards such as the one designed exclusively for e-voting, digital signature cards, the Java Card [1], the European Citizen Card (ECC), and several national eID cards, namely the Austrian, Estonian, and German eID card.

3 Systems in Use

In this section we first describe and then analyze four real-world e-voting systems using smart cards. Afterwards we define evaluation criteria, which we then use to analyse the described e-voting systems. We take both e-voting systems conducted at polling stations as well as remote e-voting into consideration. In focusing on the provided functionalities and usage of the smart cards, we chose not to focus on the parts of the system that are irrelevant to our investigation.

3.1 Remote E-voting in Austria

In 2003, remote e-voting was introduced in Austria by the research group E-Voting.at [Pr03] as a test election in conjunction with the Austrian Student Union elections at Vienna University of Economics and Business (WU Vienna). In 2004, they carried out a test election for the students at the WU Vienna during the Federal Presidential elections [Pr04] and in 2006 for Austrians abroad [PS06]. In 2009, remote e-voting was used for legally binding elections of the Austrian Student Union [Kr10]. This time a system

[1] http://www.oracle.com/technetwork/java/javame/javacard/overview/getstarted/index.html (15.02.2012)

provided by Scytl [2] was used. Remote e-voting was offered as an additional channel. Each eligible voter in possession of an Austrian citizen card [3] was able to vote over the Internet.
In accordance with §63 of [HSWO05], the Austrian citizen card has to be used to identify and authenticate voters over the Internet. The voter needs to know two PIN codes associated with his or her citizen card: PIN1 for secure electronic identification and authentication and PIN2 for using a qualified electronic signature. On an abstract level, the remote e-voting scheme works in the following way: in the first step, the voter selects the university where he or she wants to cast a vote. The voter then enters PIN1 for identification and authentication. He is then required to enter PIN2 and digitally sign his electoral registration data, thus authenticating and confirming his or her identity. The voting server checks the voter's right to vote based on the signature and the corresponding certificate and displays the corresponding ballot to the voter. Once a selection is made, the vote is encrypted by the client-side voting software. In order to cast the vote, the voter enters PIN2 again, thus signing the hash value of the encrypted vote. Afterwards, the encrypted vote and the signature are sent to the voting server.

3.2 Remote E-voting in Estonia

In Estonia, remote e-voting was first introduced for legally binding elections during the 2005 local elections and carried out again in the parliamentary elections in 2007, the 2009 European Parliament and local elections, and the parliamentary elections in 2011 [TV11, ODIHR11]. Remote e-voting was offered as an additional voting channel. Each eligible voter in possession of an ID card [4] was able to vote using remote e-voting: vote updating was enabled.

The Estonian ID card is used to identify and authenticate voters over the Internet. The voter needs to know two PIN codes associated with his ID card: PIN1 for secure electronic identification and authentication and PIN2 for using a qualified electronic signature [ODIHR11]. On an abstract level, the remote e-voting scheme works in the following way: the voter identifies and authenticates him- or herself by entering PIN1. The e-voting system checks the voter's identity and the voter’s right to vote. The voter is then provided with the corresponding ballot upon successful authentication. After having made a choice, the vote is encrypted. In order to cast the vote, the voter enters PIN2, which enables the ID to digitally sign the hash value of the encrypted vote. Once signed, the encrypted vote is sent to the voting server.

[2] http://www.scytl.com/ (15.02.2012)
[3] http://www.buergerkarte.at/ (15.02.2012)
[4] Statistics of issuing the ID card: http://www.id.ee/pages.php/03020504 (15.02.2012)

3.3 Remote E-voting for the Initiative D21 Elections

In 2003, Initiative D21 [5] was the first registered association in Germany to carry out a legally binding board election using remote e-voting. The remote e-voting system used was POLYAS [6]. Every D21 member received a PIN-protected digital signature card using a qualified electronic signature and was able to vote using remote e-voting.

In order to activate their digital signature card the voters filled out a form and sent this via fax, along with a copy of their identity card. Once voters received a confirmation email, they were able to start the voting process. On an abstract level, the remote e-voting scheme works in the following way: the voter identifies and authenticates by entering his PIN, in order to digitally sign a challenge. The e-voting system verifies the voter's identity and his right to vote by matching the voter's advanced electronic signature and email address with the one stored on the registration server. The voter then gets a random voting token, which is used to proceed with the vote casting process anonymously. Once marked, the vote is sent to the ballot box server together with the random voting token, while the transmission is secured by server side SSL.

3.4 E-voting at Polling Stations in Finland

For the 2008 municipal elections in Finland, Finnish authorities were able to arrange e-voting in three municipalities. The e-voting system in use was provided by the TietoEnator [7] company [TE08]. E-voting was offered as an additional channel and took place at polling stations. Each eligible voter who had an election-specific smart card was able to vote electronically.
After manually confirming the voter’s eligibility to vote (just the same as the traditional system), the election official configures an election-specific smart card and hands the card to the voter. The voter enables the e-voting system by inserting the smart card into the card reader. The e-voting system verifies the voter's right to vote and displays the corresponding ballot to the voter. Once the ballot is marked, the vote is encrypted by the e-voting system. The e-voting system also signs a hash value, which is derived from the encrypted vote, a random number, the voter login ID, and the election ID. The encrypted vote and the signed hash value are sent to the voting server. The voter returns the smart card to the election official, which is not used anymore in the election [KM08].

[5] D21 is a non-profit organization established in Berlin. It is Germany's largest partnership of government and industry in the information age For more information see http://www.initiatived21.de/ (15.02.2012)
[6] http://www.polyas.de/ (15.02.2012)
[7] http://www.tieto.com/ (15.02.2012)

3.5 Evaluation Criteria

In this section, we define several criteria upon which we analyze the e-voting systems described above with respect to the functionalities and usage of the smart cards [8]. The criteria are divided into three different groups: security, usability, and costs. The list of criteria used in this paper is not exhaustive, but we have chosen the same criteria used in [Vo09]:

1. Secrecy: Our definition of secrecy comprises vote-selling, secrecy of the vote, and long-term secrecy.
2. Usability: We define usability as ease of use and user-friendliness.
3. Costs: The cost factor is very important for e-voting systems, as the number of participants tends to be very high. We define costs as the total of costs for smart card readers and for smart cards.

However, before implementing e-voting systems that use smart cards, other criteria need to be taken into account as well, like robustness, time required for vote-tallying, performance, and other security requirements. Note that these criteria were defined with respect to smart cards used only for identification and authentication purposes.

3.6 System Analysis

In this section, we analyze the e-voting systems described in the previous sections by the criteria defined in section 3.5. The result of this evaluation is summarized in Table 1.

System in Use	Secrecy	Usability	Costs
Austria	+ Vote selling: the card will not be lightly passed on to a vote buyer, since this automatically means that all the other applications of this card are passed on as well	+ User-friendliness: use of the card for identification/authentication is known from other areas	+ Cost for smart cards: no extra costs, as voter already owns a card
	- Long-term secrecy: *Sig*[Hash*(*Enc(Vote))], even if the authorities are honest, the problem of long-term secrecy still remains	- Ease of use: the voter has to enter the PINs multiple times—PIN1 once and PIN2 twice.	- Costs for smart card readers: the costs of a card reader remains, if the voter does not yet possess such a device

[8] We refrain from considering integrity in this analysis as this is not addressed by smart cards.

Estonia	+ Vote selling: for the same reasons as in Austria's case - Long-term secrecy: for the same reasons as in Austria's case	+ User-friendliness: for the same reasons as in Austria's case - Ease of use: the voter has to enter two PINs	+ Cost for smart cards: for the same reasons as in Austria's case - Costs for smart card readers: for the same reasons as in Austria's case
D21	- Vote selling: in contrast to Austria/Estonia, the voter can easily sell the voting card or just the random voting token.	- User-friendliness: the voter must first learn how to use a smart card and a card reader if he or she hasn't used one before - Ease of use: the identification/authenticati on process of voters takes a long period of time	- Cost for smart cards: extra cost for the digital signature cards - Costs for smart card readers: extra costs for the card readers
Finland	- Vote selling: for the same reasons as in the case of D21, but not as easily, as the voting takes place in a polling station - Long-term secrecy: *Sig*[Hash(Enc(Vote), voter login ID...)] even if the authorities are honest, the problem of long-term secrecy still remains	- User-friendliness: for the same reasons as in the case of D21 + Ease of use: the identification/authenticati on process is fast and the e-voting system performs encrypting/signing	- Cost for smart cards: extra cost for the special voting cards - Costs for smart card readers: extra costs for the card readers

Table 1: Analysis of systems in use

The result shows that the studied systems relying on smart cards with limited functionality (electronic authentication and signing), are vulnerable to long-term secrecy. The result also shows that e-voting systems that use national eID cards (e.g. Austria, Estonia), even though these smart cards are of limited functionality, fulfil most of the criteria defined in section 3.5. The use of smart cards, which are also used in other privacy-sensitive applications (e.g. online public services, secure online banking, etc.), increases the level of security (with respect to vote selling [9]), the level of usability, and do not impose any further costs. Therefore in section 3.7, we analyze the possibility of using national eID cards with limited functionality. We investigate thereby if the problem of long-term secrecy can be eliminated without introducing new vulnerabilities.

[9] Note that there are other attacks that are not mitigated by the usage of a standard national eID. The usage of the smart card in other areas could also increase the number of possible attacks on the smart card. An attack could be started during an online-banking session, where an attacker tries to make the voter vote while the card is in "heavy" usage.

3.7 Discussion of Alternatives

The analysis of the systems under consideration revealed weaknesses regarding the integration of smart cards into remote e-voting. Based on the results of section 3.6, we investigate whether it is possible to better integrate the Austrian and Estonian national eID cards, which offer limited functionality (namely electronic authentication and signing, into remote e-voting [10]. We first describe possible scenarios to apply these cards and analyze them afterwards. To avoid attacks, like man-in-the-middle and session hijacking, only scenarios in which all communications between the client-side voting software and voting server are secured by TLS/SSL and where the server authenticates itself using its SSL certificate are considered. In case votes are explicitly encrypted, we assume that they are encrypted with the public key of the election authority and for security reasons the decryption key is shared (e.g. as described in [Ge07]). It is further assumed that some anonymization mechanisms (e.g. re-encryption mix-net [BG12]) are in place to break the link between the voter and his or her encrypted vote before decrypting votes.

We distinguish between the following three cases:

1. Two-side authenticated channel with two different voting servers (we distinguish between sending the vote as plaintext or encrypted)
    a. A registration server first checks the voter's voting eligibility based on the voter's HTTPS certificate and then provides a random voting token to the voter. The voter sends this token along with the cast vote to the ballot box server. The ballot box server checks the authenticity of the voting token and ensures that the token has not been used before. This approach is similar to the one used for the D21 elections.
    b. This case is similar to a) with the difference that the vote is sent explicitly encrypted.

2. Two-side authenticated channel with one voting server: (we distinguish between sending the vote as plaintext or encrypted)
    a. The voting server first checks the voter's voting eligibility based on the voter's HTTPS certificate and then sends him or her the ballot. The voter sends the cast vote back to the voting server secured by two-side HTTPS.
    b. This case is similar to a) with the difference that the vote is sent explicitly encrypted.

3. Digitally signing the encrypted vote:
    The voter sends the encrypted vote and a signed message to the voting server. The signed message is the hash value of the encrypted vote. The server checks the eligibility of the voter by verifying the signature. This approach is similar to the one applied in Austria and Estonia.

[10] Note that due to the limited functionality of the considered smart cards, they cannot be used to solve the problem of secure platform.

The first approach 1a is vulnerable to vote selling and coercion as the voter can forward the voting token received from the registration server. The receiver of this token can use it to contact the ballot box server and cast a vote. In addition, in scenario 1a the voter has to trust that the registration server and the ballot box server do not cooperate. The cooperation between the registration server and the ballot box server can break the election secrecy, as the voter sends his vote in plaintext. In 1b, election secrecy is ensured, even if the registration server and the ballot box server cooperate, as the vote is explicitly encrypted and due to the assumption of an anonymization mechanism; however vote-selling still remains a problem.

In 2a, the voter puts his or her complete trust in the one voting server that can break the election secrecy easily, while 2b mitigates the risk of this attack because the vote is explicitly encrypted and, due to the assumption of an anonymization mechanism, the encrypted vote is still clearly associated with the voter which causes problems with respect to long-term secrecy. However, vote-selling is not possible.

The third case is similar to the scenarios 1b and 2b: The voter has to trust the mixing process, which breaks the link between the encrypted vote and the voter's identity (his digital signature). However, signing encrypted data always recalls the problem of long-term secrecy. In addition, the voter does not see what is actually signed.

The above analysis shows that there is no better way to use smart cards, in particular national eIDs, with only limited functionality. Therefore, in section 4 we direct our attention to approaches in scientific papers using smart cards that provide more functionality.

4 Scientific Papers Based on Smart Cards with More Functionalities

In this section, we describe the different approaches of scientific papers that explore the use of smart cards that provide more functionality than only electronic authentication and signing. As many European countries have already started introducing national eID cards, we mainly focus on papers that suggest the usage of those cards. Afterwards, these approaches are analyzed. The aim of this analysis is to identify any practical, feasible functionality that might be implemented in future national eID cards with respect to e-voting. We consider both remote e-voting and e-voting in polling stations.

4.1 Remote E-voting using the European Citizen Card

The voting scheme in [Me08] is based on the design presented in [JCJ05] and its variants in [Sm05, WAB07, Sc06, AFT08]. The authors propose using the European citizen card (ECC) for the identification and authentication of voters as well as for the secure storage of voting credentials and electronic ballots. The original voting scheme is slightly modified because the ECC-standard does not support the generation of zero-knowledge

proofs or the ElGamal encryption scheme. The authors make use of the restricted identification mechanism [BSI-TR-03110] to create an anonymous election-specific identifier, and the ECC contains an additional data field as defined in [CEN1540], where an election-specific template is loaded in the registration phase. The authors argue that by using the ECC, the proposed voting scheme, which only requires linear work in the tallying phase unlike [JCJ05] (quadratic with respect to the number of votes), is receipt-free compared to [Sm05, WAB07], does not require complex zero-knowledge proofs like [AFT08], and offers an important advantage regarding usability and economic aspects.

4.2 Remote E-voting Using the German eID Card

In [BKG11], the authors propose the use of the German eID card (nPA, "neuer Personalausweis") to identify and authenticate voters making use of the restricted identification (Restricted-ID) mechanism [BSI-TR-03110] in order to create a pseudonymous election-specific identifier. At the end of the election, all of the encrypted votes and the corresponding eID server-signed restricted IDs are published on the bulletin board (BB). This information allows the public to verify the correctness of the election process, as the eID server signs only authentic restricted IDs. In [Br11], the authors argue that in [BKG11], the secrecy of the election can be broken if the eID server and the certification authority of the German eID cooperate. Therefore, the authors modified the original voting scheme, by using both the restricted-ID mechanism and a randomly generated number, the so-called votingID and blind signatures. At the end of the election, all of the encrypted votes and the corresponding anonymous votingIDs, which are blindly signed, are published on the BB. As the votingIDs are randomly generated and assigned, this ensures the secrecy of the election in contrast to the original scheme. In this case, even if the eID server and the certification authority of the German eID cooperate, they cannot break the secrecy of the election.

4.3 Votescript+

Votescript+ was first introduced in [CB09] and was developed based on the e-voting scheme presented in [Go05]. Both were designed for distributed polling stations and are based on [FOO93] and [CC96], with some improvement upon these designs. In addition, both rely on a special powerful smart card called the Java Card. The main motivation behind using Java Cards is to have smart cards with cryptographic capabilities that have been specially designed for the e-voting scheme. The authors propose using the Java Card to store and execute the vote-casting software and other data related to the voting process, including a receipt-enabling individual verification. The main difference between Votescript and Votescript+ is that Votescript+ uses two different smart cards: any national eID card for secure identification and authentication and a Java Card to run the main vote-casting application on it. The motivation behind using two different smart cards is to achieve a strong separation between the identification and authentication phase and the vote casting phase.

4.4 Votinbox

Votinbox [CS06] is an e-voting scheme designed for polling station elections. Its security relies on a smart card capable of executing cryptographic operations designed specifically for e-voting. The Votinbox e-voting scheme uses cryptographic primitives that provide anonymous services introduced in [CT04].

These cryptographic primitives are programmed into the smart card. One of the most important primitives is the list signature. This anonymous mechanism is especially suitable for e-voting, as it also provides multiple-vote detection. The cryptographic algorithms include the following: RSA encryption/decryption and signature, a secret key generator, a list signature algorithm, and a pseudo random number generator, which reproduces the same output for the same input (required by the list signature scheme).

The procedures implemented within the card help perform many functions: create a ballot, create attendance, check voting eligibility, and validate voting, which completes the participation in an election. The smart card is also able to send various data (e.g., ballot) to the voting machines. The authors argue that a key advantage of this solution is that all of the security is based on the smart card. There is also no need for an additional "Trusted Authority". This is due to the fact that by using list signatures, the participation of a signing authority during the ballot creation process is no longer required.

4.5 Analysis

In this section we analyze the scientific approaches described above according to the criteria defined in section 3.5 with respect to voter identification and authentication, storing sensitive information, securely processing parts of the e-voting scheme, and vote encryption and signing.
The work presented in [Me08] is dedicated to the integration of the European citizen card (ECC) specification with a well-studied remote voting scheme, namely [JCJ05]. Due to the restricted cryptographic capabilities of the ECC, the scheme had to be modified in order to eliminate homomorphic encryption and zero-knowledge proofs, which impose a revision of correctness and security proofs. This scheme also shares the same problem as recognized in [Br11], namely that the cooperation between the eID server and the certification authority of the ECC can break the secrecy of the election.

In the approach presented in [BKG11], the authors use the German eID card as a foundation and integrate it with a generic e-voting scheme. Their first proposal shows weaknesses due to the fact that the eID server and certification authority might break the election secrecy. While this might be acceptable for elections with low coercion risk, it is unconstitutional when it comes to legally binding elections. In a revised version of their proposal in [Br11], the authors developed the VotingID accompanied by blind signatures to ensure the secrecy of the election. While the risks of unwanted anonymity breaches can be mitigated by these measures, the voter could sell his VotingID. However, the recognized security problems in [Br11] and [BKG11] aside, another challenge to both of these approaches is how to exclude people that are not allowed to vote (e.g. people

suffering dementia or that lost their right to vote for other reasons), while still letting them use their eIDs in other areas. At this point, we recognize that the first approach has the potential to increase the level of security with respect to coercion resistance. By publishing the restricted ID associated with the corresponding vote on the bulletin board, the risk of mounting "forced-abstention" attacks can be mitigated against "less powerful" attackers, i.e., attackers that observe public channels and the bulletin board but are not able to break the used cryptographic protocols.
The concept introduced in [CB09] relies on the use of an even more powerful card than the German ID, the so-called Java Cards. From a practical point of view, this is a promising approach aimed at overcoming the drawbacks of national eID cards currently in use. However, [MP08] has shown that the flexible structure of these cards can be exploited to mount successful attacks, during which malicious code could be injected.
The concept introduced in [CS06] seems to provide some interesting functionalities that could be implemented by a smart card. However, the voting scheme is very complex, making it infeasible for real-world e-voting schemes. As an intermediate result, we commit to our prior conclusion—to rely on established smart cards for the purpose of usability and infrastructural questions.

5 Conclusion

In this paper, we examined the lessons learned for using eIDs in the context of e-voting from both existing real-world applications and scientific proposals. We first reviewed e-voting schemes in which smart cards were used to identify and authenticate voters as well as to sign votes. The sample of smart cards included both national eID cards and special purpose smart cards. The evaluation, based on the metric introduced in [Vo09], led to the conclusion that e-voting should rely on established smart cards that voters are familiar with, that do not impose additional costs, and that voters will not easily give away, thus preventing vote-selling. We further showed, that current schemes based on national eID cards, i.e., those implemented in Estonia and Austria, have weaknesses regarding long-term secrecy and require the voter to sign something that cannot read, as the message, which is signed, is encrypted. However, we showed that due to the limited functionality provided by those cards, there is no possibility to improve upon security.
Thereafter, in the second half of the paper we directed our attention to scientific proposals that focus on both, the use of national eID cards and special purpose smart cards that offer further functionalities, such as storing sensitive information (e.g. ballot, vote) and securely processing parts of the voting scheme (e.g. generate restricted ID). We discovered that national eID cards providing more functionality, like the restricted ID (pseudonym) or the German eID, have the potential to improve the security in remote electronic voting. We showed that the usage of the restricted ID can mitigate the risk of "forced-abstention" attacks.

As an overall conclusion to these lessons learned, we recommend that states that do not (yet) plan to introduce electronic voting take our considerations into account for their eID design because the proper functionality of an eID can dramatically improve the security of any e-voting system. For future work we plan to investigate the integration of

the German eID into an end-to-end verifiable and coercion-resistant e-voting scheme, while also mitigating recognized problems like secrecy of the election, long-term secrecy, and excluding "specific ineligible" voters from the election (e.g. people suffering dementia but possessing an eID). Furthermore, we direct future attention to the question of needed and offered functionality of smart cards, specifically in the field of e-voting.

Bibliography

[Ab02] Abbott, J.: Smart Cards: How Secure Are They?. SANS Institute Reading Room, 2002. http://www.sans.org/reading_room/whitepapers/authentication/smart-cards-secure-they_131 (15.02.2012)

[AFT08] Araujo, R.; Foulle, S.; Traore, J.: A practical and secure coercion-resistant scheme for remote elections. In Frontiers of Electronic Voting, number 07311 in Dagstuhl Seminar Proceedings, Germany, 2008.

[BG12] Bayer, S.; Groth, J.: Efficient Zero-Knwoledge Argument for Correctness of a Shuffle. In Advances in Cryptology – EUROCRYPT 2012 (to appear). http://www.cs.ucl.ac.uk/staff/J.Groth/MinimalShuffle.pdf (10.04.2012)

[BKG11] Bräunlich, K.; Kasten, A.; Grimm, R.: Der neue Personalausweis zur Authentifizierung bei elektronischen Wahlen. In Sicher in die digitale Welt von morgen; pp. 211-225.

[Br11] Bräunlich, K. et. al.: Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen. Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau. Nr. 11/2011. Arbeitsberichte aus dem Fachbereich Informatik.

[BSI-TR-03110] Bundesamt für Sicherheit in der Informationstechnik. Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC). Technical Directive (BSI-TR-03110), Version 2.0 - Release Candidate, 2008.

[CB09] Carracedo Gallardo, J.; Belleboni, P. E.: Use of the New Smart Identity Card to Reinforce Electronic Voting Guarantees. In Internet Technology and Secured Transactions, 2009; pp.1-6

[CC96] Cranor, Lorrie F.; Cytron, Ronald K.: Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA.

[CEN15480] Comite Europeen de Normalisation. Identification card systems - European Citizen Card - Part 1/2/3/4, 2007.

[CS06] Canard, S.; Sibert, H.: Votinbox – a voting system based on smart cards. Workshop on e-Voting and e-Government in the UK, 2006.

[CT04] Canard, S.; Traore, J.: Anonymous Services using Smart Card and Cryptography. In Smart Card Research and Advanced Applications VI – Cardis 2004, Kulwer, 2004; pp.83-98

[FOO93] Fujioka, A.; Okamoto, T.; Otha, K.: A Practical Secret Voting Scheme for Large Scale Elections, Advances in Cryptology, AUSCRYPT´92, Lecture Notes in Computer Science 718. Springer Verlag, Berlin; pp.244-251

[Ge07] Gennaro, R. et. al.; Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. In Journal of Cryptology 2007. Springer Verlag, New York; pp.51-83

[Go05] Gomez Olivia, A. et. al.: VOTESCRIPT: telematic voting system designed to enable final count verification. http://vototelematico.diatel.upm.es/articulos/Voto_telematico_Collecter_2005.pdf (15. 02. 2012)

[HSWO05] Austrian Government (Election Regulations): Hochschülerinnen- und Hochschülerschaftswahlordnung 2005. http://www.bmwf.gv.at/uploads/tx_contentbox/HSWO_2005.pdf (15.02.2012)

[ISO7816] ISO7816 Smart Card Standard: http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx (15. 02. 2012)

[JCJ05] Juels, A.; Catalano D.; Jakobsson, M.: Coercion-resistant electronic elections. In WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society; pp. 61–70

[KM08] Karhumäki, J.; Meskanen, T.: Audit report on pilot electronic voting in municipal elections, Turku, 2008. http://vaalit.fi/uploads/5bq7gb9t01z.pdf (15.02.2012)

[Kr10] Krimmer, R.: Evaluierungsbericht: E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009. Bundesministerium für Wissenschaft und Forschung, Wien, 2010.

[Me08] Meister, G. et. al.: eVoting with the European Citizen Card. In A. Brömme & al. (Hrsg.), Tagungsband „BIOSIG 2008: Biometrics and Electronic Signatures", GI-Edition Lecture Notes in Informatics (LNI) 137, 2008, pp. 67-78

[MP08] Mostowski W.; Poll E.: Malicious Code on Java Card Smart cards: Attacks and Countermeasures. In "CARDIS '08": Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications, 2008, pp. 1-16

[ODIHR11] Estonia Parliamentary Elections 6 March 2011. OSCE/ODIHR Election Assessment Mission Report, Warsaw, 2011.

[Pr03] Prosser, A., Kofler, R., Krimmer, R., Unger, M.: The first Internet-Election in Austria. Institut für Informationsverarbeitung und Informationswirtschaft Wirtschaftsuniversität Wien, Wien, 2003.

[Pr04] Prosser, A., Kofler, R., Krimmer, R., Unger, M.: Bundespräsidentschaftswahl 2004. Institut für Informationsverarbeitung und Informationswirtschaft Wirtschaftsuniversität Wien, Wien, 2004.

[PS06] Prosser, A.; Steininger, R.: An Electronic Voting Test Among Austrians Abroad. ePubWU Institutional Repository, 2006.

[RE03] Rankl W.; Effing W.: Smart Card Handbook. John Wiley & Sons, 2003.

[Sc06] Schweisgut, J.: Coercion-Resistant Electronic Elections with Observer. In (Krimmer, R. Eds.): Electronic Voting, volume 86 of LNI, pp. 171–177

[Sm05] Smith, D. W.: New cryptographic voting schemes with best-known theoretical properties. In Workshop on Frontiers in Electronic Elections 2005.

[TE08] TietoEnator Corporation: Electronic Voting Pilot 2008: Technical Implementation and Security, Version 1.1. 2008.

[TV11] Trechsel, H., A.; Vassil K.: Internet Voting in Estonia: A Comparative Analysis of Five Elections since 2005. European University Institute and European Union Democracy Observatory, 2011. http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf (15.02.2012)

[Vo09] Volkamer, M.: Evaluation of Electronic Voting. Springer-Verlag, Berlin, 2009.

[WAB07] Weber, S.; Araujo, R.; Buchmann, J.: On Coercion-Resistant Electronic Elections with Linear Work. In 2nd Workshop on Dependability and Security in e-Government (DeSeGov 2007), pp. 908–916

Session 9

New Developments and Improvements to E-voting

Electronic Voting and Null Votes: An Ongoing Debate

Marc Teixidor Viayna*

EVOL2 / eVoting Legal Lab
University of Catalonia / URV
Av. Catalunya, 35, Spain
Tarragona (Catalonia) 43002
marctv@gmail.com

Abstract: The debate over the implementation of e-voting systems still needs to respond to the question of the presence of null votes. Null votes, whose invalidity is due to a contravention of electoral norms, have become a new way through which the electors show their political discontent. The political dimension of null votes requires that e-voting systems ensure and guarantee the presence of null votes as an electoral option. Finally, it is necessary to broach the oft disputed topic of null votes attributed to technology, that is to say, the loss of valid votes due to technical malfunctions of the e-voting system and how to legally address this issue. Estonia, Australia and Norway provide useful examples when looking at technical null votes.

1 Introduction

The presence of null votes in an electronic voting system is disputed because it is necessary to decide whether we should maintain the null vote as an option in an e-voting system and how it can be implemented (§ 2-6), but there can also be some invalid votes directly attributed to technical mistakes whose legal treatment is not clear (§ 7).

In relation to this, it is necessary to first define the term *null vote* from a linguistic point of view and from a comparative legal perspective (§ 2).

* R+D Project DER2010-16741

2 Some Approaches to the Idea of a *Null Vote*

2.1 Some Semantic Precisions about the Concept

A question that needs to be asked to fully understand the concept of *null votes* is to understand that, as a legal term, it has an intensive linguistic and semantic burden, which is even more pronounced if we compare the different or similar concepts that are used for electoral implementations.

First, we need to differentiate the *null vote* from the *blank vote*. Taking the Spanish case as an example, the null vote represents a non-compliance of the formal requirements regulated by electoral law, so we can affirm that this vote is invalid, while the blank vote can be understood as a valid vote in which the elector does not manifest any political preference. The most important difference between both concepts is the valid character of a blank vote in opposition to the invalid character of the null vote[1]. This is important, because it implies that *blank votes* are computed into the tally, while *null votes* - leaving aside statistical purposes – do not enter into the final tabulation.

Secondly, *null votes* coexist with other closed terms (*spoiled vote, rejected vote*) which include a wider and more heterogeneous universe of cases than the ones included under the notion of *null vote,* but they could be used as a synonym for *null vote.* Generally speaking, a *spoiled vote* refers to a ballot that has been inadvertently damaged and handed back to the voting station officers in exchange for a new blank ballot in order to repeat the voting operation. For example, in Canada, the term *spoiled vote* implies that the voter unconsciously damages his ballot before its introduction into the ballot box[2] and can thus obtain a new ballot to vote. Furthermore, a *rejected ballot* stands for a ballot introduced into the ballot box but rejected during the counting because it is in a situation of non-compliance with the electoral rules. In the aforementioned case of Canada, for example, the term *rejected ballot* designates a ballot emitted in contravention to some electoral rules[3].

---

[1] We can't forget that some countries don't recognise the *blank vote* as an option, so in these cases, *blank votes* are actually particular cases of *null votes.*

[2] You can see the article 152 of Canada Elections Act, which contains the legal definition of *spoiled vote*: "*If an elector has inadvertently handled a ballot in such a manner that it cannot be used, the elector shall return it to the deputy returning officer who shall mark it as a spoiled ballot, place it in the envelope supplied for the purpose and give the elector another ballot".* An electronic version of the Canadian Act is available at http://laws.justice.gc.ca/eng/acts/E-2.01/page-42.html#docCont.

[3] In some cases, protest votes are shown by not marking the ballot, which is returned to the deputy returning officer and computed as a rejected ballot. In relation to the concept of *rejected ballot*, whose content is slightly more complicated, see the *Centre Poll Supervisors' Manual* (available on-line: http://www.elections.ca/res/pub/ecdocs/EC50355_e.pdf) and the *Manual on Judicial Recounts* (www.elections.ca/content.aspx?section=res&dir=loi/jud&document=jud_p3&lang=e).

Finally, and from our perspective, *null vote* refers to an intentional or unintentional contravention of electoral rules, which implies its legal inexistence and fact its non-consideration with respect to the tabulation. We can observe that the idea of a *null vote* is closely linked to the idea of a *rejected vote* because both imply a contravention of electoral rules, so they could be used as synonyms. The difference could be observed if we examine the type of contravention. For example, in Canada, one potential cause of rejection is to not mark any candidature (article 284[1] of Canada Elections Act), while in Spain this situation implies that the vote is considered blank but not null. Although the definitions of the *null vote* and the *rejected vote* are very similar, the type of contravention or the content covered by both notions could be different, but ultimately, it is a country's legislation that defines a *null vote*.

2.2 The Legal Treatment of the Null Vote: A Brief Explanation of the Spanish, Italian, and French Cases

In the case of Spain, the null vote is regulated in article 96 of the General Elections Act (1985). Its first paragraph establishes that the vote is null when cast with an unofficial ballot layout or envelope. It is also considered null when cast with no envelope or when the envelope contains more than one ballot. Secondly, the norm establishes that nullity also includes modifying, adding, or deleting candidates' names and altering the order of candidates. Moreover, the introduction of any expression, crossing out, or other voluntaries alterations will also produce the nullity. Finally, the precept establishes for the case of the Senate, where open lists apply, the nullity of votes in which the voter had chosen more candidates than the maximum number legally allowed.

From a jurisprudential perspective, the judicial and constitutional criterion in order to address the question is the principle of the non-alterability of the ballot. It is a jurisprudential[4] criterion so it is not literally picked from the law; however the content of article 96.2 implies an indirect recognition of such a principle. As far as the electoral ballots contain closed lists that cannot be modified by the elector – except in the particular case of the Senate – no modifications or additions to the electoral ballot are allowed. Otherwise, the elections could hinder the free exercise of the right of suffrage, which is an indispensable cornerstone in the democratic system (see Pu07). Moreover, according to the line adopted by the Venice Commission, we can say that the "freedom of voters to express their wishes primarily requires strict observance of the voting procedure"5.

---

[4] The Constitutional Court, for example, on its judgement 168/2007, on July 18th, declared the nullity of a ballot on which the elector drew a cross near the name of one parliamentary candidate. The Court understood that the contravention of the principle of non-alterability of the ballot was clear. Also, the judgment 165/1991, on July 19th, understands that written, underlined, marked or crossed ballots should be considered as null votes. The judgement 169/2007, on July 18th, declared nullity in the case of two ballots which presented a cross near the name of the first candidate of the list because it wasn't possible to determine if the elector desired to reject the first candidate or not.

[5] See *Code of Good Practice in Electoral Matters*, adopted by the Venice Comission (july-october 2002). The electronic format of the Code is available at http://www.venice.coe.int/docs/2002/CDL-AD%282002%29023-e.pdf.

In Italy, the idea of the null vote as an invalid ballot is recognised both in the elections to Senate and to the Congress of Deputies. In the case of the *Camera*, the voter can only choose one of the lists presented for elections which figures on the ballot. If he or she wants to vote correctly, the elector must mark the corresponding box and is not allowed to make any other type of mark or expression (art. 58 DPR 361/1957). Article 4 of DPR 361/1957 establishes the impossibility of express preferences. As can be seen, rage in Italy is also submitted to rigid, formal rules whose contravention entails the vote's nullity[6]. In the case of Senate the situation is practically identical (art. 14 Legislative Decree 533/1993).

Finally, French law provides another useful example. The null vote as a vote that won't be computed is recognised in article L-66 Electoral Code. From the point of view of the French legislator, a null vote (*vote nul)* is understood as a ballot that contains insulting references to candidates, a ballot or an envelope with expressions or signs, a vote expressed by a non-official envelope or ballot, or finally ballots printed on colored paper. Also, an envelope that contains more than one ballot from different political options nullifies the vote (art. L-65 of Electoral Code). As the article L-66 says, these null votes won't be taken into consideration in order when the result is being tallied. Article L-57 of Electoral Code, which contains several provisions in relation to the expression of votes through electronic means, is also particularly relevant. The norm ensures the presence of blank votes, but nothing is said in relation to null ones.

3 Types of Null Votes: a Political Differentiation

In connection with all we said, from a political perspective, we can distinguish between two types of null votes. First, we can refer to null votes which are produced by inexperience or voter error (e.g. a voter who marks four Senate candidates when only three can be chosen). Secondly, we can refer to votes whose nullity is not due to unintentional formal errors.

The nullity of such votes is produced by an intentional decision which has an inescapable political content: the voter finds a way through which he can show his political disagreement versus the system through the non-application of norms[7]. In other words, *unintentional null votes* are produced by a voter error that could be avoided if the

[6] See the official document *Manuale elettorale: le norme per le elezione politiche*, which is available at the website of the Italian Deputies Congress: http://www.camera.it/view/doc_viewer_full?url=http%3A//www.camera.it/application/xmanager/projects/camera/attachments/upload_file/upload_files/000/000/004/MANUALE_11marzo2008.pdf&back_to=http%3A//www.camera.it/363%3Fconoscerelacamera%3D33

[7] Spain provides an extremely interesting example in the context of 2009 Basque elections, where there were roughly 100000 null votes (8,84% of cast votes), as a protest against the illegalization of a *nationalist* political party. As a matter of fact, some politicians of this party encouraged the citizens to show their disagreement through the nullity, and the advice was actually seconded. The party even printed non-valid ballots with the same layout as the official ones which were brought to the voters who supported the party. See www.elpais.com/articulo/espana/100000/vascos/respaldan/opcion/voto/nulo/Batasuna/elpepiesp/20090302elpepinac_8/Tes.

voter knew that the ballot was about to be cast incorrectly. *Intentional null votes* are those whose illegality is already recognized by the voter, but the voter decides to show his discontent through this wrong formal procedure.

In the latest Spanish elections (November 2011), the total amount of null votes was tracked. For example, in the case of the Lower Chamber, the two latest Spanish general elections have shown relevant data. In 2008 the percentage of null votes was 0.64%, with a participation of 73.85%. In 2011, the percentage of null votes increased to 1.29% with a minor decrease in participation, which was at 71.69%8. From 2008 to 2011, the percentage of null votes increased 0.65 points, just the double of 2008. This phenomenon, in our opinion, might have a political significance: the null vote is understood by voters as a way to express a rejection of politics or a political protest. The case of the Senate is more accentuated: the number of null votes jumped from 2.29% (2008) to 3.71% (2011), an increase of 1.42 points[9].

We can assume that society has given an additional political significance to the null vote[10], which coexists with the traditional vision of the null vote as a product of a mistake or error during the voting process: the voters show their discontent through the vote's nullity. The ideal of democratization is extended and includes the null vote as an authentic form of a voter's political preference, which should be protected and guaranteed. For ROUSSEAU,, the ideal of democracy consists of the direct expression of the general will, which should be expressed directly and without representation (see Ra10: 71-79): the null vote could be a form to express some aspects of the general will directly, and it also could be an expression of the *freedom of opinion,* through which the politicians can be made aware of the views of the citizenry (see Ma97: 206-215).

---

[8] These electoral data were published by the Spanish Government and they are available on-line: (http://elecciones.mir.es/resultadosgenerales2011/99CG/DCG99999TO_L1.htm).

[9] See the official report of the Spanish Government at: http://elecciones.mir.es/resultadosgenerales2011/99pdf/CS11-DOSSIER.pdf

[10] In some cases, the role of blank ballots as "protest votes", whose objective is to show the elector's discontent with the system and politicians, has been replaced by null votes, probably due to the different legal treatment between null votes and blank votes. Taking the Spanish case as an example, blank votes are valid inputs in order to calculate the legal barrier from which a political formation can obtain parliamentary seats, while null votes wouldn't be considered in this sense. As a matter of fact, the elector knows that null votes generally would not be interpreted with the poisonous meaning– from a legal point of view – with which the blank votes would be. Politics and some political analysts tend to give to blank votes a politic charge; that is to say, they tend to interpret that the blank vote probably could be a punishment to one party or to one ideological position, when the blank vote might actually be a protest against the overall system. Moreover, the elector usually knows that blank votes generally benefit big parties, which are in fact the parties in relation to which the political discontent is normally greater. The null vote with its unlawful character easily rejects interested interpretations and does not benefit big parties.

4 E-voting Procedures: the F*ate* of the Null Vote

One of the achievements of e-voting, which is commonly alleged as an advantage by most suppliers, is precisely the re-motion of null votes11. If we only consider null votes as a mistake or an error, any system ensuring that this kind of error cannot take place will be welcomed.

However, we stated before that null votes can be considered as an error, but they can also be considered as a deliberate protest. In the first case, the re-motion of null votes can be valued as an authentic benefit, but, in the second case, it is difficult to affirm to what extent the elimination of a political preference is helpful or desirable. Actually it does mean an attenuation of the chances to express a given political opinion. Curiously enough, this issue could entail that a supposed advantage, as is the elimination of null votes, can be considered as a disadvantage at the same time because it implies a reduction in the freedom of expression. In our opinion, the null vote option as a protest ballot should be present on any e-voting platform. It could be a way to strengthen the right to suffrage and a chance to bring to politicians and governments a new way through which they can be made aware of the citizen's perception about the political system. From a pragmatic point of view, we can also say that null votes do not damage the traditional content of the right to suffrage: on the contrary, they reinforce the democratic features of the system[12].

The issue has not yet received mainstream attention from legal literature. For RENIU VILAMALA, the elimination of null votes by e-voting systems "is acceptable and desirable insofar as it eliminates accidental null votes (…) but is counter productive for another type of null vote: deliberate null vote" (see Re08: 142). Indeed, these null votes contain an "authentic rejection of all the candidates" (Re08: 142) or political options which concur to elections, or even a renunciation in order to take part in the electoral process, because the elector does not find any desirable political option or he or she wants to show dissatisfaction with the system. A similar opinion is defended by MARTÍNEZ DALMAU, who underlines the potential contradictions between e-voting systems and null votes as an expression of a political preference. Naturally, e-voting systems, which are based on automation and which, technically, only validate proper election procedure could not allow null votes (see Mar06: 35-37; Mar10: 74).

[11] For example, the E-Verification Project (Electronic Verification for presential e-voting systems), which is managed by CRISES – University Rovira i Virgili and Scytl, remarks that "E-voting helps on reducing or almost preventing the existence of null votes". The quotation is literally picked from http://crises-deim.urv.cat/everification/index.php. See http://jcel.unizar.es/jcel07/ponencias/JCEL_Voto_Electronico.pdf (page 7/33).

[12] Obviously not all countries recognize the presence of intended null votes in their electoral legislations. The introduction of the null electronic vote as we explained, that is to say, as a protest vote due to an intentional voter decision, is a desirable objective for any e-voting system.

After all, the question is still whether null votes should have a place as a political option (which can be chosen by the voter) in a hypothetical implementation of e-voting systems[13]. BARRAT ESTEVE understands that the minimum content of the right *to suffrage* covers the existence of blank votes as well as null votes (see Ba07: 38). For FERNÁNDEZ RODRÍGUEZ the existence of null votes is something desirable from a political perspective because their meaning is clear (see Fe07a: 31): the nonexistence of the null vote lessens the voter's capacity to express political options (see Fe07b: 312). The democratic legitimization of electoral systems "includes the free expression of the preferences of the voter, even through casting a non-valid or a white paper ballot" (Mi03: 51), so in e-voting systems, "in order to preserve the freedom of voter decision, the possibility for casting a consciously invalid vote must be provided and guaranteed" (Mi03: 51). However, other authors, like PRESNO LINERA, understand that the null vote is not covered by the right to suffrage because *stricto sensu* the null vote is not a way to make political decisions nor to draft legal norms (see Pr07: 357-358).

5 E-voting Procedures: How Can We Cast a Null Ballot?

As stated, a number of authors think that it is necessary to preserve the null vote as a political option in a hypothetical e-voting system. We will now analyse the way in which null votes may exist in an e-voting system. From our point of view, as initial sketches, two ways could be considered[14].

The first way (i) is merely choosing the option of null vote. Just as other candidatures from different political formations exist, the null vote would also be recognised as an electoral option.

With the purpose of making it real, it is necessary that the electronic interface displays, among the list of candidatures or political options, the null vote as an option on the voting interface, otherwise, the right to suffrage and democratic legitimacy could be undermined.

Following this path, the design of the system should satisfy two requirements:

a. It is necessary to visually distinguish between the options of voting for a certain political ideology from the two possibilities through which the elector does not choose any option (the blank vote and the null vote). This differentiation should be clearly, directly, and fairly visualized, that is to say, with no hidden collateral options.

[13] In general, see the work of Guido Schryen at http://www.e-voting.cc/static/evoting/files/schryen_p121-131.pdf and the work of Patricia Heindl at http://www.e-voting.cc/static/evoting/files/heindl_p165-170.pdf.

[14] *Napasandi*, India is an interesting case because the right to reject is recognized by e-voting machines. With such a right to reject, a voter can say he does not want to vote for any of the candidates. See the piece of new at: http://www.firstpost.com/politics/annas-unique-lingo-what-is-napasandi-254869.html.

b. Moreover, the electronic interface should inform the elector about the sense of blank votes and null votes, in order to ensure that the voter has sufficient knowledge to vote correctly. Even though the traditional regulation of paper-based votes does not do so, it would be an opportunity to strengthen the elector's knowledge.

The second way (ii) in which the null vote can be expressed is the possibility to write something down on the *electronic ballot.* If null votes, within a traditional electoral system (leaving aside the case of non-deliberate null votes), express a protest, the nullity as a political option in an e-voting system would only be guaranteed if the elector also has the opportunity to write down whatever he or she desires. In some cases, the protest is ordinarily displayed as a message written down on the ballot, so a similar possibility of expression should be guaranteed by an e-voting system. In the end, this option adds the possibility to show the reasons for the disagreement to the first one.

However, it is clear that this option would normally be limited due to important operational barriers. In order to rationalize the possibility, we can point out some considerations:

a. The timeframe during which the elector decides his/her vote must be limited. It is a rational requirement; otherwise, the election could become paralysed and even technical security concerns may arise. The voter should have enough time to express his or her opinion, but the timeframe should obviously be reasonable enough in order to preserve the order of election and its correct development15. Once that timeframe has elapsed, the marked ballot will automatically be sent out, and the voter may not change the ballot's content. The idea of a temporal limitation is particularly relevant in the context of physically e-voting at a polling station because that timeframe can easily become a crippling factor. The voting machine will be used by a lot of people and a single voter, misusing his or her right, can damage the rights of the rest. The case of Internet voting is totally different since the voter does not need to go to a polling station; therefore it is more difficult for the voter to damage the rights of other people, but technical security concerns are still valid if not greater.

b. The message should also be limited in relation to its length because the idea is to express his or her rejection.

Due to usability problems, the voter might face problems in correctly casting a null ballot by using the written option (e.g. the application might end before the elector can write all that he or she desired). In the precedent case, the problem could be attributed to the inexperience of the voter, not to the system; we cannot forget that this kind of vote will be also counted as a null vote, despite the fact that the elector would not have been able to add a personal expression to his vote.

[15] For example, 2 or 3 minutes, enough time in order to write down a protest message.

6 Null Votes Attributed to Technology: a Legal Rigmarole

Null votes can also be generated by technical malfunctions, that is to say, not linked to the voter's behaviour. In this hypothesis, the elector believes that the ballot has been properly cast– and actually it was–, but the system somehow loses track of the ballot so it does not make into the final tally. Despite the technical explanations that can be provided, it is worth wondering which legal treatment should be applied should this occur. Given that they may have different features, the next paragraphs will provide a quick overview of three different cases [Estonia (i), Australia (ii) and Norway (ii)] when the system has unexpectedly generated null votes.

The first case was generated during the Estonian parliamentary elections in 2011[16] (i). The ODHIR Report recalls that "during the counting, one vote was determined invalid by the vote counting application, since it was cast for a candidate who was not on the list in the corresponding constituency. The project manager could not explain how this occurred"[17]. As any other similar failures, one can find two initial explanations depending on the origin of such a mistake: a successful external attack that managed to alter the content of the electronic ballots or perhaps an internal error that led to an improper layout of the candidates. The first option might have two reasonable origins as well since the hacker could be the voter him/herself or an outsider; the legal consequences of either option would be significantly different. If the voter wants to hack the system and if he or she manages to vote for the wrong candidates, as happened in Estonia, there is an easy and non-problematic legal solution since such a ballot would be sorted as invalid. Voters also used to alter the content of paper ballots and such hacking would only be a new and updated version of these traditional null votes. The invalidity of this vote would reflect the actual will of the voter. Obviously, if the system does not detect this hacking, we would be faced with a great problem, not linked to null votes.

The other two pending hypotheses (i.e. successful hacking conducted by outsiders or an internal mistake due to backend problems) are much more challenging because the voter would not know that his or her ballot was declared invalid. Electoral authorities are responsible for the correct layout of the ballot and the electoral procedure may not delegate such a task to each voter. If the ballot includes a wrong candidate or if it allows other invalid actions, such as making multiple selections for the same candidate when preferential voting is applied, there is a legal assumption that the correct ballot and the voter will obviously have no responsibility.

Despite the different approaches that each hypothesis needs, it is worth stressing that Estonian authorities failed to provide a detailed explanation, that is to say, they were assuming that, beyond the theoretical explanations that could justify what happened, there were not enough data to determine the actual origin of the failure. Given that we have three different scenarios, and only one of them complies with democratic principles, one can legitimately assume that such illegal explanations might have been

[16] For a general overview of the constitutionality of the Estonian e-voting system, see MV11: 5-7.

[17] See the Report of the *Office for Democratic Institutions and Human Rights (ODIHR)*, which is available on-line: http://www.osce.org/odihr/77557.

the correct one or at least that it has to be taken into account as a potential danger. As a consequence, if no valid argument is provided, such null votes uncover external hackings as well as insider mistakes, which cannot be excluded when e-voting systems are deployed. Obviously, such a conclusion may seriously undermine the overall legitimacy of these new voting channels.

A similar case took place in Australia (ii), during the 2011 New South Wales elections. It was observed that an output file of the votes did not appear to agree with the number of votes actually printed. The official explanation is that the *java script* allowed the introduction of non-numeric characters to be entered as ballot preferences, an atypical failure which affected 43 ballots. Although this misconfiguration could be easily corrected, the remote causes of the failure are still unknown to electoral authorities.

As a matter of fact, the situation is similar to the Estonian case because the causes of such failure could indicate a hacker attack or an internal system error. When speaking about an internal failure, or an external attack not initiated by the voter, the legitimacy of the e-voting system could be undermined and obviously citizen confidence could decline significantly[18].

We find in Norway another two hypotheses (iii) of technical null votes. While the first one is very similar to what has already been analysed for Estonia[19] and Australia, there is also a curious new sort of null ballot. As explained during the final counting ceremony[20], a voter managed to cast his or her ballot during the very last second of the voting session, which lasted 30 minutes for to security reasons, but the ballot arrived to the ballot box a few moments after the timeframe expired. Consequently, when the ballot box was cleansed, that meant deleting all ballots that would not be used in the tally (e.g. ballots belonging to people who died before the final election day), the concerned vote was also deleted even though it was correctly cast within the legal timeframe.

It must also be noted that the voter received a so-called return code, that is to say, an SMS text message sent to each voter to confirm how she or he had voted. Return codes intend to guarantee individual verifiability so that each voter is able to prove that his or her ballot has been received as cast and cast as intended.

From a legal point of view, there are some doubts as to how to categorize such a ballot. First of all, it is worth stressing that this ballot did not reach the tally stage. As it is known, the so-called counting ceremony included three different, separate steps: cleansing, mixing, where the ballots break the sequence that they had, and tallying.

---

[18] A brief explanation of the Australian incident is available at: http://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/93481/iVote_Audit_report_PIR_Final.pdf

[19] See the OSCE/ODIHR report at http://www.osce.org/odihr/88577.

[20] See video of the counting ceremony held in Oslo in September 12th 2011 (minutes 53:21, 57:48 and 1:00:05). See the video at the following link: http://media01.smartcom.no/Microsite/dss_01.aspx?eventid=6316

The ballot was rejected during the first step because it was considered as a ballot that had not reached the ballot box in time and theoretically it should receive the same legal treatment as other ballots that had also been rejected, for other reasons, by the cleansing server. However, such a solution does not seem reasonable because the other rejected ballots always had a correct basis. The rejected ballot might have been cancelled by the same voter with another vote or it might belong to a person who was no longer entitled to vote. Therefore the system may take into account these rejected ballots, but only for statistical purposes, as it actually did during the counting ceremony. There is no democratic argument that requires these ballots to be included in the final, official results because they are not expressing any citizen's will.

However, such an approach is not valid for our problematic ballot. It does express the legitimate will of a given citizen, and it cannot be merged with other ballots whose rejection is only due to management reasons. Although already deleted during the cleansing, this problematic ballot would need to be included as a technical null vote in the final record of the official results. Moreover, when computing the turnout, this voter should also be included as he or she had correctly cast the ballot, only technical reasons prevented its inclusion in the final count.

7 Conclusions

The implementation of e-voting systems should protect and guarantee the presence of null votes as one supplementary electoral option because the nullity, which consists in a contravention of the electoral rules, may be deliberately used as a way in which the elector shows his or her political discontent. From our point of view, two ways could exist to realize the null vote option in the context of an e-voting system: first, the null vote could be included with other options in the electronic interface and secondly the precedent option might also include a personal written statement, as it has always been the case in traditional paper-ballot systems.

Finally, it is absolutely necessary to debate the legal treatment of null votes attributed to technological failures, which still is an open question. Estonian, Australian and Norwegian e-voting systems made presented real problems and each one has interesting different features that have subsequent legal consequences. Given that such technical incidents can seriously damage the citizens' trust in e-voting systems, legal frameworks would have to properly process these scenarios determining, if possible, their different origins. While a successful external hacking would not be a legal problem, provided it was discovered, an internal misconfiguration may create more doubts, namely when it is misleading for the voter, who may believe that his or her ballot has been correctly cast and processed.

Bibliography

[Ba07] Barrat Esteve, J.: Viabilitat del vot electrònic des de la perspectiva politicojurídica. In: (Barrat Esteve, J. et al.): El vot electrònic a Catalunya: reptes i incerteses. Mediterrània, Barcelona, 2007.

[Fe07a] Fernández Rodríguez, J. J.: Democracia y nuevas tecnologías: aproximándonos al voto electrónico. In: (Fernández Rodríguez, J. J. et al.): Voto electrónico. Estudio comparado desde una aproximación jurídico-política. Funda*p*, Mexico, 2007.

[Fe07b] Fernández Rodríguez, J. J.: El voto electrónico: sus garantías y posibilidades de regulación. In: (Cotino Hueso, L. Coord.): Democracia, participación y voto a través de las nuevas tecnologías. Comares, Granada, 2007.

[GR11] Gálvez Muñoz, L. A; Ruiz González, J. G.: El voto electrónico y el test de calidad; o de cuatro bodas complicadas y un posible funeral. In: Revista de Derecho Político, 2011(81)

[Ma97] Manin, B.: Los principios del gobierno representativo. Alianza Editorial, Madrid, 1997

[Mar06] Martínez Dalmau, R.: Electronic vote, democracy and participation. Vadell Hermanos Editores, València, 2006.

[Mar10] Martínez Dalmau, R.: Democracia y voto electrónico. In: (Carracedo, J. D. Coord.): Democracia digital, participación y voto electrónico. Ediciones del CEPS, València, 2010.

[Mi03] Mitrou, L.; Gritzalis, D.; Katsikas, S.; Quirchmayr, Gerald: Electronic voting: constitutional and legal requirements, and their technical implications. In: (Gritzalis, D. Ed.): Secure Electronic Voting. Kluwer Academic Publishers, London, 2003.

[MV11] Madise, Ü.; Vinkel, P.: Constitutionality of remote internet voting: the Estonian perspective. In: Juridica International: Law Review. University of Tartu, 2011(18).

[Pr07] Presno Linera, Miguel Ángel: La globalización del voto electrónico. In: (Cotino Hueso, L. Coord.): Democracia, participación y voto a través de las nuevas tecnologías. Comares, Granada, 2007.

[Pu07] Pulido Quecedo, M.: Bromas y veras en materia electoral. Actualidad Jurídica Aranzadi, núm. 738/2007 (http://www.westlaw.es).

[Ra10] Ramírez Nárdiz, A.: Democracia participativa. La democracia participativa como profundización de la democracia. Tirant lo Blanch, València, 2010.

[Re08] Reniu Vilamala, J. M.: Doubts and certainties about electronic voting. In: (Reniu Vilamala, J. M. Ed.): E-voting: the last electoral revolution. Institut de Ciències Polítiques i Socials, Barcelona, 2008.

A Fair and Robust Voting System by Broadcast

Dalia Khader[1], Ben Smyth[2], Peter Y. A. Ryan[1], and Feng Hao[3]

[1]Universite du Luxembourg, SnT,
Luxembourg
{dalia.khader | peter.ryan}@uni.lu

[2]Toshiba Corporation,
Kawasaki, Japan
toshiba@bensmyth.com

[3]Newcastle University
Newcastle, United Kingdom
Feng.hao@newcastle.ac.uk

Abstract: Hao, Ryan, and Zieliński (2010) propose a two-round decentralized voting protocol that is efficient in terms of rounds, computation, and bandwidth. However, the protocol has two drawbacks. First, if some voters abort then the election result cannot be announced, that is, the protocol is not robust. Secondly, the last voter can learn the election result before voting, that is, the protocol is not fair. Both drawbacks are typical of other decentralized e-voting protocols. This paper proposes a recovery round to enable the election result to be announced if voters abort, and we add a commitment round to ensure fairness. In addition, we provide a computational security proof of ballot secrecy.[1,2]

1 Introduction

Paper-based elections derive security properties from physical characteristics of the real world. For example, marking a ballot in isolation inside a polling booth and depositing the completed ballot into a locked ballot box provides privacy; the polling booth also ensures that voters cannot be influenced by other voters, and the locked ballot box prevents the announcement of early results, thereby ensuring fairness; and the transparency of the whole election process from ballot casting to tallying alongside the impossibility of altering the markings on a paper ballot sealed inside a locked ballot box gives an assurance of correctness and facilitates verifiability. Moreover, the combination of these physical constraints ensures a robust voting scheme. Replicating these attributes

[1] Smyth's work was partly done at Loria, CNRS & INRIA Nancy Grand Est, France as part of the ProSecure project, which is funded by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n0258865, and the ANR-07-SeSur-002 AVOTE project. Khader & Ryan conducted their work as part of the SeRVTS-C09/IS/06 project, funded by the FNR.

[2] This paper has been published in Word format after conversion from Latex. We have tried to eliminate the errors introduced during this conversion process, however, we suspect some errors remain. Accordingly, we refer the reader to the LaTeX created document, which is available on the authors' web pages.

in a digital setting has proven to be difficult and, hence, the provision of secure electronic voting systems is an active research topic, first inspired by Chaum [Cha81].
Two classes of e-voting systems can be distinguished: (i) Decentralized e-voting systems, where voters run a multi-party computational protocol without any additional parties, for example [Sch99, KY02, Gro04, HRZ10] and (ii) Centralized e-voting systems, where election administrators run the election, for example [JCJ05, XSH+07, RT09]. Decentralized systems are typically designed for small-scale elections with a focus on security with minimal trust assumptions; whereas, centralized schemes are typically designed for large-scale elections and rely upon stronger trust assumptions to enable scalability, usability, and robustness. In this paper we focus on decentralized voting schemes.

Kiayias & Yung [KY02], Groth [Gro04] and Hao, Ryan, and Zieliński [HRZ10] have come to a consensus that the following properties are essential for decentralized voting schemes:

- Perfect ballot secrecy: A voter's vote is not revealed to anyone else, modulo what can be computed from the published tally.
- Self-tallying: At the end of the protocol, voters and observers can tally the election result from public information.
- Fairness: Nobody has access to partial results before the *deadline*. The precise definition of deadline varies in the literature. In this paper, we suppose fairness is satisfied if no one has access to partial results before casting their vote. (Note that our definition would permit a voter to abort the protocol after having observed partial results but could not change their vote.)
- Dispute-freeness: A scheme is dispute-free if anyone can verify that the protocol was run correctly and that each voter acted according to the rules of the protocol.

In addition, we also consider *robustness*.

- Robustness: A corrupt voter cannot prevent the election result from being announced.

Hao, Ryan, and Zieliński [HRZ10] propose an election scheme, which makes some progress toward satisfying these properties. However, their scheme is neither robust nor fair: in particular, a single voter can prevent the election result from being announced and the last voter can cast her vote with full knowledge of the election result.

1.1 Contribution

We propose a variant of the Hao, Ryan, and Zieliński [HRZ10] election scheme that ensures fairness and robustness, and we formally prove ballot secrecy using provable security techniques.

2 Preliminaries

This section presents the assumptions and cryptographic primitives that will be used to construct our scheme. We shall start with some notations and conventions used throughout the paper. Let $\mathcal{H}$ denote a hash function and (p, q, g) be cryptographic parameters, where p and q are large primes such that $q|p-1$ and g is a generator of the multiplicative subgroup of $\mathbf{Z}_p^*$ of prime order q. In some of our security proofs we rely on the assumption that the Decisional Diffie-Hellman (DDH) problem is hard, which is a logical consequence of using ElGamal-style encryption as a building block for our protocol .

Definition (Decisional Diffie-Hellman problem)

Given integers $g^a, g^b, g^c \in \mathbf{Z}_p^*$ *and* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{Z}_q^*$ are chosen randomly.

The distribution $\{(g, g^a, g^b, g^{ab})\}$ *is computationally indistinguishable from* $\{(g, g^a, g^b, g^c)\}$.

Our scheme is reliant on signatures of knowledge to ensure secrecy and integrity and to ensure voters encrypt valid votes; we now recall suitable primitives.

2.1 Knowledge of Discrete Logs

Proof Statement: Proving knowledge of x, given h where $h \equiv g^x \bmod p$ [CEGP87, CEG88, Sch90][3].

Sign: Given x, select a random nonce $w \in_R \mathbf{Z}_q^*$ and compute

- Witness $g' = g^w \bmod p$
- Challenge $c = \mathcal{H}(g') \bmod q$
- Response $s = w + c \cdot x \bmod q$.

Output Signature (g', s)

Verify: Given h and signature (g', s), check $g^s \equiv g' \cdot h^c \pmod p$, where $c = \mathcal{H}(g') \bmod q$.

A valid proof asserts knowledge of x such that $x = \log_g h$, i.e., $h \equiv g^x \bmod p$.

[3] The challenge can also include the ID of the participant to prevent replay attacks such that $c = \mathcal{H}(\mathbf{ID} || g^{\mathbf{r}}) \bmod q$

2.2 Equality Between Discrete Logs

Proof Statement: Proving knowledge of the discrete logarithm x to bases $f, g \in \mathbf{Z}_p^*$, given h, k where $h \equiv f^x \bmod p$ and $k \equiv g^x \bmod p$ [Ped91, CP93].

Sign: Given f, g, x, select a random nonce $w \in_R \mathbf{Z}_q^*$. Compute

- Witnesses $f' = f^w \bmod p$ and $g' = g^w \bmod p$
- Challenge $c = \mathcal{H}(f', g') \bmod q$
- Response $s = w + c \cdot x \bmod q$.

Output signature as (f', g', s)

Verify: Given f, g, h, k and signature (f', g', s, c), check $f^s \equiv f' \cdot h^c \pmod p$ and $g^s \equiv g' \cdot k^c \pmod p$, where $c = \mathcal{H}(f', g') \bmod q$.

A valid proof asserts $\log_f h = \log_g k$, i.e., there exists an x such that $h \equiv f^x \bmod p$ and $k \equiv g^x \bmod p$. This signature of knowledge scheme can be extended to a disjunctive proof of equality between discrete logs (see below.)

2.3 Disjunctive Proof of Equality Between Discrete Logs

Proof Statement: Given that $(a, b) = (g^x, g^{y-x} \cdot g^m)$ contains message m, prove that $m \in \{min, \ldots, max\}$ for some parameters $min, max \in \mathbf{N}$, where $min < \max$ [CGS97, CDS94].

Sign: Given (a, b) such that $a \equiv g^x \bmod p$ and $b \equiv h^x \cdot g^m \bmod p$ for some nonce $x \in \mathbf{Z}_q^*$, where plaintext $m \in \{min, \ldots, max\}$.

For all $i \in \{min, \ldots, m-1, m+1, \ldots, max\}$, compute challenge $c_i \in_R \mathbf{Z}_q^*$, response $s_i \in_R \mathbf{Z}_q^*$, and witnesses $a_i = \dfrac{g^{s_i}}{a^{c_i} \bmod p}$ and $b_i = \dfrac{h^{s_i}}{\left(\dfrac{b}{g^i}\right)^{c_i} \bmod p}$.

Select a random nonce $w \in_R \mathbf{Z}_q^*$. Compute witnesses $a_m = g^w \bmod p$ and $b_m = \boldsymbol{h}^w \bmod p$,

challenge

$$c_m = \mathcal{H}(a, b, a_{min}, b_{min}, \ldots, a_{max}, b_{max}) - \sum_{i \in \{min, \ldots, m-1, m+1, \ldots, max\}} c_i \pmod q$$

and response $s_m = w + x \cdot c_m \bmod q$.

To summarize, we have

- Witnesses $(a_{min}, b_{min}), \ldots, (a_{max}, b_{max})$
- Challenge $c_{min}, \ldots, c_{max}$
- Response $s_{min}, \ldots, s_{max}$

Output signature of knowledge (a_i, b_i, c_i, s_i) for all $i \in \{min, \ldots, max\}$.

Verify: Given (a, b) and $(a_{min}, b_{min}, c_{min}, s_{min}, \ldots, a_{max}, b_{max}, c_{max}, s_{max})$, for each $min \leq i \leq \max$ check $g^{s_i} \equiv a_i \cdot a^{c_i} \pmod p$ and $\boldsymbol{h}^{s_i} \equiv b_i \cdot \left(\frac{b}{g^i}\right)^{c_i} \pmod p$.

Finally, check. $\mathcal{H}(a, b, a_{min}, b_{min}, \ldots, a_{max}, b_{max}) \equiv \sum_{min \leq i \leq max} c_i \pmod q$.

A valid proof asserts that (a, b) contains the message m such that $m \in \{min, \ldots, max\}$.

3 Voting Scheme

In this section, we present a variant of the Hao, Ryan, and Zieliński [HRZ10] election scheme, which guarantees fairness without any computational overhead and, moreover, we introduce a recovery procedure to ensure robustness.

In [HRZ10, Gro04, KY02] the authors assume authenticated public channels to prevent a participant from voting multiple times and to ensure eligibility of voters: we adopt the same assumption.

3.1 Toward Fairness

In this section, we extend the Hao, Ryan, and Zieliński [HRZ10] protocol to include an additional *Commitment Round* to ensure fairness.

Given a number of voters $n \in \mathbf{N}$, the scheme proceeds as follows:

Setup Round: Each voter $i \in n$ selects a private key $x_i \in_R \mathbf{Z}_q^*$ and computes the corresponding public key $a_i = g^{x_i} \bmod p$. Each voter has to prove that a_i has been constructed correctly by proving knowledge of x_i (§2.1).

Commitment Round: Each voter $i \in n$ computes h_i as follows.

$$h_i = g^{(x_1+\cdots+x_{i-1})-(x_{i+1}+\cdots+x_n)} = \frac{\prod_{j=1}^{i-1} a_j}{\prod_{j=i+1}^{n} a_j}$$

The voter constructs $b_i = h_i^{x_i} \cdot g^{v_i}$, where $v_i \in \{0,1\}$ is the voter's vote.
A disjunctive proof of equality between discrete logarithms $\log_{\top g} [\![a_{\downarrow} i]\!] = \log_{\top}(h_{\downarrow} i) [\![b_{\downarrow} i]\!]$ and $\log_{\top g} [\![a_{\downarrow} i]\!] = \log_{\top}(h_{\downarrow} i) [\![b_{\downarrow} i]\!] / g$ is computed to prove that $v_i \in \{0,1\}$ (§2.3). Note that the signature includes challenge c_{v_i}, which acts as a computationally binding commitment to values a_i and b_i. Furthermore, the value b_i is not published in this round.

Voting Round: Each voter publishes b_i .

In the above protocol description, the pair (a_i, b_i) is an ElGamal-style encryption of the voter's vote, where v_i is the plaintext, x_i is a nonce, and h_i is the public encryption key; ballot secrecy is ensured because no coalition can recover a voter's vote.

As an alternative to the above commitment round, a voter could publish a hash of the values output during the voting round in [HRZ10], however, we have observed that the signature of a knowledge scheme has a computationally binding and computationally hiding commitment to the vote v_i since the value b_i is hashed among the other elements of the signature of knowledge. Thus, a hash of the values output in the voting round in [HRZ10] is not necessary.
In [HRZ10] the last voter can vote having complete knowledge of the election result. This limitation is avoided in our scheme with an additional round, more precisely, the commitment round and the voting round correspond to a single voting round in [HRZ10]. The separation of rounds exploits the result by Cramer *et al.* [CFSY96] (Lemma 1). Namely, no partial results are available during the commitment round in order to ensure Fairness.

Lemma 1: The signature of knowledge produced during the commitment round demonstrates $v \in \{0,1\}$ without releasing the actual value of v .

Once all voters have completed the protocol, the self-tallying property allows the election result to be derived by observers and voters.

Self-Tallying: Given some protocol output such that all the signatures of knowledge hold the result $v \log_g V$, where V is defined below:

$$V = \prod_{i=1}^{n} b_i = \prod_{i=1}^{n} h_i^{x_i} \cdot g^{v_i} = g^{\sum_{i=1}^{n} v_i}$$

In our scheme, the result v is the sum of the votes for 1; the votes for 0 can be trivially derived as $n - v$.

Formally, the computation $v \log_g V$ follows from Proposition 2, as shown by Hao, Ryan, and Zieliński. Although the computation of the discrete logarithm is hard in general, we know that the election result v is such that $1 \leq v \leq n$ and, therefore, the search for the value v is feasible with complexity of $O(n)$ by linear search or $O(\sqrt{n})$ using the Pollard-Lambda [Pol00] or baby-step giant-step algorithm [Sha71] (see also [LL90,3.1]).

Proposition 2:
Given integer $n \in \mathbf{N}$, we have for all $x_i \in \mathbf{Z}_q^*$ and $y_i = (x_1 + \cdots + x_{i-1}) - (x_{i+1} + \cdots + x_n)$ the $\sum_{i=1}^{n} x_i \cdot y_i = 0$.

3.2 Robustness

In the protocol by Hao, Ryan, and Zieliński a voter can prevent the election result from being announced by aborting. In this section, we introduce an efficient *recovery round* to enable the election result to be announced even if voters abort. Moreover, our recovery round maintains the security of the scheme; in particular, no votes can be modified or revealed during the recovery round.

Let us suppose $\mathcal{L}$ is the set of voters that submitted valid ballots in the voting round, where $|\mathcal{L}| < n$, that is, a subset of voters either did not vote or submitted an invalid signature of knowledge. A recovery round can be executed as follows to allow the election result to be announced:

Recovery Round: Each voter $i \in \mathcal{L}$ computes $\widehat{h}_i$ as follows:

$$\widehat{h}_i = \frac{\prod_{j \in \{i+1,\ldots,n\} \setminus \mathcal{L}} a_j}{\prod_{j \in \{1,\ldots,i-1\} \setminus \mathcal{L}} a_j}$$

Each voter publishes $\widehat{h}_i^{x_i}$ together with a signature of knowledge asserting $\log_{\tau g} [\![a_i]\!] = \log_{\tau}(\hat{h}_i) [\![\hat{h}_i^{\tau}(x_i)]\!]$ (§2.2).

In the recovery round, the outputs $\left\{ \widehat{h}_i^{x_i} \middle| i \in \mathcal{L} \right\}$ act as cancellation tokens during tallying to eliminate the need for private keys of voters whom did not participant in the voting round (see Table 1 for a simple illustration).

No	First round	Second round	Third round	Recovery
1	g^{x_1}	commitment	$g^{x_1 y_1} = g^{x_1(-x_2 - x_3 - x_4 - x_5)}$	$\widehat{h}_1^{x_1} = g^{x_1(x_2 + x_4)}$
2	g^{x_2}	commitment	Abort	--
3	g^{x_3}	commitment	$g^{x_3 y_3} = g^{x_3(x_1 + x_2 - x_4 - x_5)}$	$\widehat{h}_3^{x_3} = g^{x_3(x_4 - x_2)}$
4	g^{x_4}	commitment	Abort	--
5	g^{x_5}	commitment	$g^{x_5 y_5} = g^{x_5(x_1 + x_2 + x_3 + x_4)}$	$\widehat{h}_5^{x_5} = g^{x_5(-x_2 - x_4)}$

Table 1. Example of recovery: With no loss of generality, we assume $n = 5$ and all participating voters send ``no'' votes. Also, we have omitted the mention of ZKPs, as it is not needed for this illustration. Notice that data sent in the recovery round cancel out the effects of the drop-outs from the final tallying.

Suppose $\mathcal{L}'$ is the set of voters that broadcast valid values in the recovery round such that $\mathcal{L}' = \mathcal{L}$, then the self-tallying property allows the election result to be derived by observers and voters; otherwise, another recovery round is required by voters $\mathcal{L}'$.
Given the output of the recovery round for all voters $\mathcal{L}$, such that all the signatures of knowledge hold, the result is $v = \log_g V$, where V is defined below:

$$V = g^{\sum_{i \in \mathcal{L}} v_i} = \prod_{i \in \mathcal{L}} \hat{h}_i^{x_i} \cdot h_i^{x_i} \cdot g^{v_i} = \prod_{i \in \mathcal{L}} \hat{h}_i^{x_i} \cdot b_i$$

Once again, the result v is the sum of the votes for 1.
Formally, the computation $v = \log_g V$ follows from Proposition 3.3.

Proposition 3.3:
Given the integer $n \in \mathbb{N}$ *and set* $\mathcal{L} \subset \{1, \ldots, n\}$,
we have for all $x_i \in_R \mathbb{Z}_q^*$, $y_i = (x_1 + \cdots + x_{i-1}) - (x_{i+1} + \cdots + x_n)$

$$\hat{y}_i = \sum_{j \in \{i+1, \ldots, n\} \setminus \mathcal{L}} x_j - \sum_{j \in \{1, \ldots, i-1\} \setminus \mathcal{L}} x_j$$

and

$$\sum_{j \in \mathcal{L}} (x_j \cdot y_j) + (x_j \cdot \hat{y}_j) = 0$$

that .

Proof:
We have

$$\sum_{j \in \mathcal{L}} (x_j \cdot y_j) + (x_j \cdot \hat{y}_j) = \sum_{j \in \mathcal{L}} x_j \cdot (y_j + \hat{y}_j)$$

and

$$y_j + \hat{y}_j = \sum_{k \in \{1, \ldots, j-1\} \cap \mathcal{L}} x_k - \sum_{k \in \{j+1, \ldots, n\} \cap \mathcal{L}} x_k$$

.

Note that if a voter decides $|\mathcal{L}|$ is too small to maintain privacy (e.g., when $|\mathcal{L}| = 2$), then she can decide not to join the recovery round and abort; in this case, the voter obtains an assurance of ballot secrecy (under the DDH assumption), but her vote is not included in the tallying procedure, i.e., her vote is discarded.

Discussion: Re-running an Election is not Equivalent to Recovery.
Critics may argue that the recovery round is not necessary because elections can be efficiently re-run. However, two runs of an election protocol do not gaurantee the same result and this may lead to attacks. For example, suppose there is a referendum to decide whether electronic voting should be adopted.I In this setting, opponents of electronic voting could force a re-run of the referendum in the hope that the system's failure to announce the election result in the first run will sway the electorate's opinion in a re-run. This can occur in [HRZ10]. For example, all voters behave honestly except Mallory, who forces a re-run and thus has the opportunity to influence the opinion of the electorate; moreover, Mallory can plausibly deny that she is malicious, for example, by claiming that she dropped her laptop and lost her key.

3.3 Multi-Candidate Voting Scheme

We adopt the technique used in [HRZ10] to extend our scheme to multi-candidate elections. Assuming we have n voters and k candidates. A value m is chosen such that it is the smallest integer where $2^m > n$. The main modification to handle multi-candidate elections is during the voting round: the voter's choice is $v_i \in \left\{2^{0}, 2^{(k-1)}, \ldots, 2^{(k-1)m}\right\}$.

The setup and recovery rounds are unchanged. The commitment round uses a signature of knowledge (§2.3) where $min = 2^0$ and $max = 2^{(k-1)m}$.

The tallying will cause $V = g^{\sum_{i=1}^{n} v_i} = g^v$, however $v = 2^0 c_0 + 2^{(k-1)} c_1 + 2^{(k-1)2} c_2 \ldots + 2^{(k-1)m} c_{k-1}$, where c_j is the number of votes that went for candidate j for any $j \in \{0, \ldots, k-1\}$. The value $v \leq 2^{(k-1)m} n$ can be efficiently computed (the maximum value is if all voters vote for the last candidate) using a baby-step giant-step algorithm (this is possible because the values of k tend to be small), and $c_1, \ldots, c_k$ can be recovered using the super-increasing nature of the encoding with the help of algorithms such as the knapsnack algorithm.

4 Security and Performance Analysis

This section presents a computational security proof of ballot secrecy (§1) and compares our scheme with existing decentralized voting protocols in the literature (§2).

4.1 Ballot Secrecy

Hao, Ryan & Zieliński [HRZ10] provide strong arguments to show that ballot secrecy is satisfied in their scheme under the DDH assumption.
In this work we add a formal proof of Ballot Secrecy using provable security techniques and game models, assuming honest-but-curious voters. This implies participants are honestly creating the input of the protocol but curious to know the others' inputs. This assumption is a common practice [Gro04]. Under this assumption, the signatures of knowledge can be dropped from the game model. This game model is for proving ballot secrecy. Since these signatures of knowledge reveal minimum information, the first signature reveals one bit proving knowledge of x_i; the signatures of knowledge in the commitment and voting round reveal that v_i belongs to a set of values (the adversary already knows this set); and the last signature reveals another bit proving equality of x_i to the bases $g, \hat{h}_i$. None of the information revealed by the signatures of knowledge is related to the final value of the vote in an interesting manner. In our game model, we allow the adversary to query an oracle $CrptVoter(i)$ where the challenger responds with x_i.

Ballot Secrecy (BS-Security): We say a decentralized voting scheme is BS-Secure, if no polynomially-bounded adversary $\mathbb{A}$ has a non-negligible advantage against the challenger $\mathbb{C}$ in the following ballot secrecy game:

- Set-up Round: $\mathbb{C}$ chooses all x_i and publishes all g^{x_i}, for $i \in \{1, \dots, n\}$
- Challenge: The adversary chooses voters j and k that have not been queried in $CrptVoter$. The challenger randomly chooses one of j, k to have voted as 1 and the other as 0. We refer to the voter who voted 1 as pv. The challenger randomly chooses $pv \in \{j, k\}$ to vote 1 and the remaining voter to vote 0.
- Voting Round: The adversary can call for the voting round to start. The adversary gets to vote on behalf of the corrupted voters. Furthermore, the adversary gets to abort certain voters causing the need for a recovery round to be executed; he can select the voters to abort.
- Recovery Round: If a voter aborts, then the recovery round is executed. The adversary is permitted to select voters to abort during the recovery round, forcing the recovery round to be re-run.
- Guess Phase: The adversary outputs a $guess \in \{j, k\}$.

The adversary $\mathbb{A}$ may query the oracle $CrptVoter(i)$, with the restriction that $i \in \mathbb{A}\{j,k\}$just after the game is setup and until the guess phase.

To win the game the adversary must select $guess \in \{j,k\}$ such that $guess = pv$ with a probability greater than guessing, we say that ballot secrecy is satisfied when this is not the case.

Definition 1, *(Ballot Secrecy Security):*

The voting scheme is BS-Secure if for all polynomial time adversaries, the $Pr|guess = pv| - \frac{1}{2} \leq \epsilon$ „ ϵ is negligible.

Now we show that if an adversary who can win the game above exists, then there exists a simulator that can break the DDH Problem. We shall prove the following theorem via contradiction.

Theorem 2: If there exist an adversary that wins the BS model above, then there exist a simulator that can solve the DDH problem.

Proof.:

Assume we have a tuple g^a, g^b, g^c where $c \in \{ab, random\}$. The simulator assumes $a = x_k$ and $b = x_j$. For the setup round the values $g^{x_k} = g^a$ and $g^{x_j} = g^b$ are submitted. Simulating the vote round is done as follows:

- For (v_k, v_j): The simulator tosses a fair coin of $\{0,1\}$, v_k is equal to the output of the coin and v_j is the opposite value.
- For (x_k): Simulator needs to compute $g^{x_k y_k} g^{v_k}$. The value g^{v_k} is simple to compute given the previous coin toss. Compute:

$$g^{x_k y_k} = g^{a y_k} = g^{a\left(\left(x_1 + \cdots + x_{k-1}\right) - \left(x_{k+1} + \cdots + x_n\right)\right)}.$$
$$g^{x_k y_k} = (g^{a x_1} . g^{a x_2} \ldots g^{a x_{k-1}} . g^{-a x_{k+1}} \ldots g^{-a x_n}).$$

  Note that all values of x_i are known to the challenger except x_j , and the simulator replaces the term $g^{a x_j} = g^c$. This becomes a valid input in the voting round if and only if $c = ab$. The same technique can be used to run the recovery round. If $c = ab$, then the round would be simulating the real protocol, regardless of the number of times the round is executed.
- For (x_j): Simulator performs the same computations as for x_k and replaces the term $g^{a x_k} = g^c$.

If $c = ab$ and, given the assumption that there an adversary that wins the privacy game exists, then the adversary will definitely return the right value among $\{j, k\}$ and the simulator will guess that $c = ab$, but if the adversary of the privacy game aborts, then $c = random$.

Note that the same proof can be extended to hold for multi-candidate schemes

4.2 Performance Comparison

We compare our scheme with existing decentralized voting protocols (Table 1). It is immediately apparent that our scheme provides better performance than [KY02] and [Gro04], and we add an additional round in comparison with [HRZ10], this additional round is introduced to achieve fairness.

Protocol	[KY02]	[Gro04]	[HRZ10]	Our scheme
Rounds	3	n+1	2	3
Exponentials	2n + 2	4	2	2
Knowledge of d.logs	n + 1	2	1	1
Equality of d.logs	n	1	0	0
Disjunctive equality of d.logs	1	1	1	1

Table 2: Performance summary per voter

Performance of Recovery: We omit the cost of the recovery round from Table 2 since the other schemes are not robust. The additional costs associated with recovery are as follows: one additional exponential and one additional equality of d.logs, per voter, per round.

Performance of Multi-Candidates: The scalability of the schemes in Table 2 to multi-candidate elections are all similar. In our scheme, the additional computation during the commitment round is linear to the number of candidates and self-tallying requires execution of the Knapsnack algorithm.

Optimisations: We highlight two optimizations**:**

1. In [HRZ10, Gro04, KY02] the authors assume that each voter has a one-way authenticated broadcast channel. This assumption was made for two reasons: to detect a voter who is casting more than one vote and to ensure that only eligible voters can vote. One might be able to relax this assumption: authenticated channels are only needed in the first round. Under this assumption, the signatures of knowledge can be used to ensure that security is preserved in later rounds, in particular, witness that the value a_i (implicitly implying x_i) has been used in every round of the protocol and also during tallying; it should follow that authentication of a_i is sufficient for security. This could be achieved by authenticating the first round only. We therefore think the assumption that all communication must use authenticated channels might be relaxed in our protocol and in the protocol proposed in [HRZ10]. The savings associated with this weaker assumption are dependent upon the implementation of an authenticated channel and studying this optimization remains as a possibility for future work.
2. Let us consider a variant of our scheme with two rounds: the voter sends the ballot during the commitment round. If all voters participate in two rounds, then we have the original scheme [HRZ10]; in this case, fairness is not provided. However, if one voter completes three rounds, then fairness is provided, as we shall now argue: Let $\{x_1, \ldots, x_n\}$ be the private keys of voters. Suppose voters publish $b_1, \ldots, b_{k-1}, b_{k+1}, \ldots, b_n$ during the commitment round (as per the original scheme [HRZ10]) and the remaining voter only publishes her signature of knowledge. Self-tallying the published ballots produces the following:

$$V = \prod_{i=1, i=\not k}^{n} b_i = \prod_{i=1, i=\not k}^{n} h_i^{x_i} \cdot g^{v_i} = {b_k}^{-1} g^{\sum_{i=1}^{n} v_i} = h_k^{-x_k} \cdot g^{-v_k} g^{\sum_{i=1}^{n} v_i}$$

Witness that no partial election result can be derived from V without b_k, hence fairness is achieved assuming one voter completes three rounds of the protocol.

5 Conclusion

We present a fair and robust variant of the decentralized electronic voting protocol proposed by Ryan & Zieliński [HRZ10], and prove that our scheme satisfies perfect ballot secrecy under the DDH assumption. Moreover, our scheme is self-tallying and dispute-free. Furthermore, we have shown that our scheme is efficient when compared to existing decentralized voting schemes from the literature.

Bibliography

[CDS94] Ronald Cramer, Ivan Damga˚rd, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In CRYPTO'94, volume 839 of LNCS, pages 174–187. Springer, 1994.

[CEG88] David Chaum, Jan-Hendrik Evertse, and Jeroen van de Graaf. An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations. In EUROCRYPT'87, volume 304 of LNCS, pages 127–141. Springer, 1988.

[CEGP87] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf, and Rene´ Peralta. Demonstrat- ing Possession of a Discrete Logarithm Without Revealing It. In CRYPTO'86, volume 263 of LNCS, pages 200–212. Springer, 1987.

[CFSY96] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-Autority Secret-Ballot Elections with Linear Work. In EUROCRYPT'96, volume 1070 of LNCS, pages 72–83. Springer, 1996.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In Eurocrypt, pages 103–118. Springer- Verlag, 1997.

[Cha81] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24:84–90, February 1981.

[CP93] David Chaum and Torben P. Pedersen. Wallet Databases with Observers. In CRYPTO'92, volume 740 of LNCS, pages 89–105. Springer, 1993.

[Gro04] Jens Groth. Efficient Maximal Privacy in Boardroom Voting and Anonymous Broadcast. In FC'04, volume 3110 of LNCS, pages 90–104. Springer, 2004.

[HRZ10] Fao Hao, Peter Y. A. Ryan, and Piotr Zielin´ ski. Anonymous voting by two-round public discussion. Journal of Information Security, 4(2):62 – 67, 2010.

[JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-Resistant Electronic Elections. In Proc. of Workshop on Privacy in the Electronic Society (WPES05), Alexandria, VA, USA - November 7, 2005, pages 61–70, 2005.

[KY02] Aggelos Kiayias and Moti Yung. Self-tallying Elections and Perfect Ballot Secrecy. In PKC'02, volume 2274 of LNCS, pages 141–158. Springer, 2002.

[LL90] Arjen K. Lenstra and Hendrik W. Lenstra Jr. Algorithms in Number Theory. In Jan van Leeuwen, editor, Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity, chapter 12, pages 673–716. MIT Press, 1990.

[Ped91] Torben P. Pedersen. A Threshold Cryptosystem without a Trusted Party. In EURO-CRYPT'91, number 547 in LNCS, pages 522–526. Springer, 1991.

[Pol00] John M. Pollard. Kangaroos, Monopoly and Discrete Logarithms. J. Cryptology, 13(4):437–447, 2000.

[RT09] Peter Y. A. Ryan and Vanessa Teague. Pretty Good Democracy. In Proc. of the 17th Security Protocols Workshop, Cambridge, UK, 2009, LNCS. Springer, 2009.

[Sch90] Claus-Peter Schnorr. Efficient Identification and Signatures for Smart Cards.In CRYPTO'89, volume 435 of LNCS, pages 239–252. Springer, 1990.

[Sch99] Berry Schoenmakers. A Simple Publicly Verifiable Secret Sharing Scheme and its Ap- plication to Electronic Voting. In CRYPTO'99, volume 1666 of LNCS, pages 148–164. Springer, 1999.

[Sha71] Daniel Shanks. Class number, a theory of factorization and genera. In Number Thory Institute, volume 20 of Symposia in Pure Mathematics, pages 415–440. American Mathematical Society, 1971

[XSH+ 07] Zhe Xia, Steve Schneider, James Heather, Peter Y. A. Ryan, David Lundin, Roger Peel, and Philip Howard. Preˆt a` Voter: All-In-One. In Proc. of the IAVoSS Workshop On Trustworthy Elections (WOTE 2007), June 20-21, 2007

Mobile Voting as an Alternative for the Disabled Voters

H. Serkan Akilli[1]

Department of Public Administration
Faculty of Economics and Administrative Sciences
Nevsehir University
2000 Evler Mah. 50300, Nevsehir, Turkey
h.serkanakilli@nevsehir.edu.tr

Abstract: The aim of this presentation is to highlight the common problems disabled voters have during elections and to emphasize the importance of mobile voting in creating a more inclusive, participatory democracy. Results of a qualitative textual analysis of a web-based forum about the experiences of disabled citizens during the 2009 local government elections are used to identify the legal, physical, and emotional problems associated with participating in elections. In the final section, the results of a questionnaire, which was e-mailed to disabled voters, are presented, and it is argued that establishing a mobile voting system for disabled voters may bypass many of the problems affecting this community and that mobile voting may be more efficient when compared to other solutions. It is often suggested that trust building and extensive public relations activities should be designed to prepare the society for new types of voting, and pilot work is recommended for those who need these innovations the most—disabled voters.

1 Introduction

Representative democracy is about representatives who act on the behalf of those who elected them. However, we cannot talk about democratic representation wherever elections have been held. The elections must exhibit universally recognized qualities in order to be labeled democratic. Basically, they need to be general (universal suffrage), free, fair, and secret. Although elections date back to ancient history, these qualities were only achieved after popular struggles in the late 19th century and spread across Europe in the early 20th century. The right to vote was hard to win. People were required to provide information concerning who they were, what their income was, how much tax they paid, or even details about their racial background before they were granted their basic rights as citizens. In some Western democracies, blacks and women were only allowed to vote in the second half of 20th century. Still, free, fair, and anonymous elections seem out on the horizon in many parts of the world.

[1] An earlier version of this paper comparing young voters and disabled voters was presented at the EGOVSHARE 2009 Conference, Antalya, Turkey.

Winning the right to vote is one thing, but using, or being able to use this right is another? Today, the biggest concern for governments in developed democracies is to increase voter turnout and ensure that every citizen is able to express his or her will at the ballot box. Although there are various legal arrangements in Europe and in Turkey to make it easier for people who have difficulty reaching polling stations, accessibility remains problematic for some sections of society like the elderly or people with disabilities. In the search for more inclusive democracies, technological developments offer valuable instruments such as remote polling via computers, mobile phones, or cable televisions. But these innovations are not without problems, and there is need for extensive work before being able to fully benefit from their potential. Along these lines, this paper focuses on mobile voting and its usability for disabled voters.

Thanks to developing mobile technologies, exciting opportunities have flourished in the public sector. Various services including emergency response, the police force, tax payment, and car parking information are only a few of the mobile services that governments have started to provide for their citizens. However, the implications of these innovations are not limited to public services. From a political perspective, it is not too early to talk about the emergence of *mobile democracy*. Mobile democracy can be defined as using mobile interfaces to improve the relationship between the government and its citizens, and it connotes a move toward a more inclusive and participatory democracy. Of course it would be an exaggeration to claim that democratic ties between the governments and its citizens may be strengthened only with the help of mobile communication devices [BB03]. However, the potential benefits for both parties carry too much promise to be neglected. Mobile devices can reach a great majority of citizens, cutting across dualisms such as wealth, gender, education, age, and regional development level [Ge04] [Ny05]. New types of networks may erode traditional information flow hierarchies and provide fast and effective ways to disseminate and mobilize information [Ca06] [Sr05] [He08] [Su06]. Mobile technologies offer constituents the opportunity to closely monitor their governments, and they provide voters with a channel for being heard [KK04]. On the other hand, governments, political parties, and NGOs would have access the people much more easily than traditional communication channels allow. Thus, it would not be wrong to say that it is crucial to establish the necessary substructures for the coming age of M-democracy and that there is a need to begin pilot schemes to identify country-specific problems as soon as possible.

As the core element of representative democracy is the election, it is logical to say that mobile voting, which can be defined as voting via mobile devices, should be considered one of the most important drivers of mobile democracy. Although an exciting idea, various countries' experiences have proven that mobile voting has many issues that need to be solved before it can be utilized for large-scale elections. It is evident that social, legal, technical, and political problems may pose serious challenges against mobile voting [Bo07] [Sc03] [Jo02] [Lo02] [Mo03]. Furthermore, since many democracies are suffering from ever-declining voter turnouts [GC00], decreasing party memberships [MB01], and distrust in institutions and politicians [Pu00] it is evident that democratic governments need to modernize participation channels according to the changing lifestyles of their societies in order to reach as many citizens as possible.

In this paper, it is argued that disabled voters should be the first group of citizens to test the feasibility of mobile voting in Turkey because a large portion of the approximately *four million* disabled voters face innumerable difficulties during an election, ensuring that their political wills are hardly reflected at the ballot box. In order to develop this argument, the first section provides brief information on relevant election regulations concerning disabled voters. The second section highlights common problems faced by disabled voters throughout an election. The third section discusses whether mobile voting could be a viable solution for disabled voters in the light of data obtained from a questionnaire that was e-mailed to disabled voters.

2 Election Regulations Concerning Disabled Voters

Turkey is a representative democracy and, as previously mentioned, there are legal arrangements to ensure free, fair, and anonymous elections for every citizen just as other European countries. According to the Turkish Constitution, every citizen who is older than 18 has the right to vote in elections and on referendums. However, the Constitution and the Law of the Essential Provisions of the Elections and the Elector Rolls (henceforth the Electoral Law), list those who cannot vote and those who cannot be a voter. Soldiers (excluding officers), military students, and prisoners cannot vote in elections, while the incapacitated and those who have been denied public service cannot register. Thus, disabled citizens have elective franchise rights just as any other citizen so long as they meet the necessary requirements.

Articles 36, 74, 90, and 93 of the Electoral Law establish the rules for disabled voters. According to the Article 36 if the voter has a disability, which does not allow the voter to vote, it must be noted during electoral registration. The Article 74 is about the duties of the ballot box commission. It is the responsibility of the commission to "make necessary arrangements to make disabled voters vote comfortably". The Article 90 says that "pregnant, sick, and disabled voters cannot be kept waiting" at the voting queue. According to Article 93 "the blind, the paralyzed, or those with *clearly apparent* physical disabilities may cast their votes with the help of one of their relatives who is from the same constituency or any voter in the absence of any relatives". However, a voter is not permitted to help more than one disabled voter.

When the aforementioned regulations are considered, it is seen that rule makers have tried to overcome the difficulties that may prevent the disabled voters from expressing their political wills at the ballot box. However, as in many areas of life, the actual experiences of disabled voters during an election prove the need for further legislation. In the following section, election day for a disabled voter is depicted using discussions from an Internet forum whose members are either disabled or close friends/family members of disabled citizens.

3 Election Day for a Disabled Voter

One of the advantages of the Internet has been its ability to connect people around the world regardless of race, religion, gender, or any other differences. The Internet has become a fertile place where social networks, friendships, and even social movements blossom faster and participants express themselves more freely than in the real world. Thus, the Internet may be considered a good starting point to investigate the true feelings and opinions of particular social groups.

In this section, the most common legal, physical, and emotional problems that the disabled voters face during the elections are highlighted by using the results of a qualitative textual analysis of a web-based forum[2] about the experiences of the disabled citizens at the latest local government elections. The forum has 21,000 members who are either themselves disabled or are close friends/family members of disabled citizens. The members have different types of disabilities, so it is possible to spot common problems rather than problems associated with a specific type of disability.

Four discussion topics on the forum were selected in order to collect data about the election experiences of the disabled voters. The topics are titled "Place: Republic of Turkey, Event: Local Government Election of 2009, The Victims: The Disabled, Offender: Higher Election Committee", "Political Rights: The Disabled Citizens Who Have Been Denied Their Right to Vote", "Proposal about the Architectural Problems That Restrict Disabled Voters". Forum members talk about their.experiences as pertaining to these four topics,

Four sub-headings are used to illustrate the election day of disabled voters. These include: "Transportation To the Voting Area", "Reaching the Ballot Box", "Casting the Vote", and "Overall Effect of the Election". The experiences of the disabled voters at the election day are discussed at length to highlight what benefits mobile voting would foster.

3.1 Transportation to the Voting Area

The challenges of the election start with the task of reaching the voting area from the residence of the disabled voter. In this phase, we can make an initial distinction between two groups of disabled voters. We can distinguish one group of disabled voters who can leave their houses with or without the help of other people (family members, friends, etc.) or special equipment (wheel chairs, hearing devices, etc). The second group of disabled voters includes those who cannot even leave their houses due to their disabilities.

[2] www.engelliler.biz

The first group of disabled voters may be considered luckier because their chances of voting, as will be mentioned below, are much higher than the second group. However, the road to the polling station has its own problems. Besides the usual architectural obstacles such as stairs and unsuitable pavements, we can spot particular problems due to the election regulations. First of all, the distance of the voting location determines the type of transportation options. If the voting area is close to the disabled voter, she/he may choose to travel without using public/private transportation, which is less problematic option. However, if the voting location requires transportation, problems start to emerge. In some cases, political parties or NGOs provide transportation for the disabled voters (including voters in elderly care institutions), but this service is often strictly tied to a promise to vote for a particular party and explicitly illegal. Since the law does not allow public institutions to use their resources during elections to prevent influence, municipalities cannot allocate their vehicles, which are also not always suitable for disabled people, to provide transportation for the disabled voters who do not have private transportation opportunities.

The second group of disabled voters, those who cannot leave their houses due to their disabilities, face more difficulties than the first group. The first, and less important, problem for these citizens is the election fine. According to the law, the registered voters who do not vote at elections must pay a fine. However, if the voter can prove that she/he has a legal excuse not to vote, the fine may not be enforced[3]. Therefore, it could be said that when the disabled voter does not wish to vote, since she/he cannot reach the voting area, there should be no problem at all. However, if she/he wishes to vote, the regulations fall short. According to the law, the voter must cast his/her vote in person and cannot appoint a proxy to vote on his or her behalf. Although forum members explain that their relatives had voted on behalf of them in previous elections, this rule seems to have been more strictly enforced in the latest election. In the forum, one of the voters said that he had been voting by proxy for years and had never had a problem. However, in the latest local elections, the Higher Election Commission (YSK) ruled that the disabled voters may not appoint a proxy to vote for them, and those who have already been appointed a guardian (about 400.000 voters) were not sent their voter papers[4].

It is not possible to appoint election officers to visit the houses of those voters who cannot leave their houses due to their disabilities either. Thus, there seems to be no option for them to vote, and it is obvious that some type of remote voting method should be considered for those disabled voters who have the ability to vote but do not have the opportunity to do so.

---

[3] Although the election fine has been an instrument to stimulate voter participation, it has not been implemented to this date due to the cost of the process. However, during the presidential and local elections, the government signaled an increase for fines.

[4] It should be noted here that not all of these 400000 citizens are incapacitated in terms of civil law or law of obligations. They need a guardian only for daily transactions such as personal care, banking or shopping since they cannot leave their houses.

3.2 Reaching the Ballot Box

Once the disabled voter reaches the voting area, there remains the arduous task of getting to the ballot box. Many of the ballot boxes are placed at schools that have multiple stories, and many of these schools, which have been designed for *healthy,* young students, do not have proper accessibility options (elevators etc.) for the disabled voters. So there are two alternatives: either the voter may be carried to the ballot box with the help of other voters, or the ballot may be brought to the voter.

Each of these solutions has its own limitations. Some types of disabilities, having fragile bones for example, require special handling, which strangers may not be able to provide without hurting the voters, or perhaps it would be too embarrassing for the disabled voters to ask strangers to carry them to the voting room[5]. This first option is also open to influence, since in some places, members of political parties offer to help disabled voters (of course not without acknowledging their political affiliation), thus breaching election restrictions.

Bringing the voting paper to the disabled voter is an informal solution, and it cannot be done without violating multiple regulations. For example, it is forbidden to take the voting seal out of the polling station, and votes should be cast under the inspection of the ballot box commission. In such cases, the chairmen of the ballot box commission use personal judgment to allow the paper to be sent to the voter, yet this is not regulated clearly. Since the *necessary arrangements* for the disabled voters to vote comfortably, as mentioned in the law, are tied to the personal judgment of the chairman on the ballot box commission, different chairmen may reach different conclusions about similar situations. This variety in practice frequently leads to harsh arguments between the disabled voters and the election officers.

Lack of information about the different types of disabilities may sometimes lead the chairmen to make insufficient decisions too. For example, one of the forum members explains that the chairman of the ballot box did not believe that he was 97% disabled as he did not see anything externally wrong with the voters (since the disability of the voter was not *clearly apparent* as mentioned in the law).

The forum participants also complain that the ballot box commissionaires may be quite anxious due to fear of allegations of fraud or official complaints of other parties' representatives, and thus they do not give permission to send the paper to the voter.

[5] According to the forum members, this is especially a greater problem for the young female voters. One of the young female forum members tells that she was too embarrassed to be carried by her father, while another member says he was able to vote but it was much harder for his sister, and that they do not think she will vote in the next election.

3.3 Casting the Vote

At the zenith of the voting process, voters are expected to use a seal, which is stamped onto the voting paper. This is also not an easy thing to do for some of the disabled voters. For instance, blind, spastic, paralyzed, and amputee voters need help to cast their votes. The regulations allow one relative of the disabled voter or one voter from the same ballot area to help. However, in this case, the secrecy of the vote is being lost, and the disabled voter may not be able to assert her/his real will due to the pressure of the bystander (the helper may cast the vote as she/he wishes or manipulate the voter)[6].

3.4 Overall Effect of the Election

The forum members provide a clear picture of the election's end. Some members of the forum were able to vote without any difficulty since they were enrolled at an accessible polling station located on the first floor of a school. Some of them feel they were lucky just to reach the ballot box, even though their votes had been improperly cast, violating election regulations. While others say, they had been too embarrassed or frustrated that they do not think they will ever bother casting a ballot again. Those who were not able to vote, feel that they have been denied their right to vote, and hence their right to be an active citizen; they believe that none of the political parties or public institutions, including the Higher Election Commission, are willing to solve their problems.

It would not be an exaggeration to say that the elections, which represent the pinnacle of the democratic process, may turn into a nightmare for many disabled voters. Such experiences may lead to the further isolation and alienation of these citizens, and naturally, these problems should not be neglected in a proud democracy.

4 Is Mobile Voting a Viable Option for Disabled Voters?

In this section, the viability of mobile voting for disabled voters in Turkey is discussed with the help of the results of a questionnaire, which was e-mailed to forum members. The sample set consisted of approximately 40 disabled people; therefore, the data are not well suited for extrapolation and making generalizations. However, they may be used to provide clues about some of the obstacles facing mobile voting. In the future, there is certainly a need for a large-scale, and if possible, comparative work in different political cultures about disabled voters' attitudes about remote voting types.

Before analyzing the opinions of the disabled voters about mobile voting, it would be beneficial to provide some information on the responses of disabled voters when asked an open-ended question about what proposals they had for helping disabled citizens during elections. The most frequent answer to this question was architectural

[6] A visual impaired respondent writes that if mobile voting should be possible, the blind voters would at last be 100% sure of which party they voted for.

accessibility. Fourteen respondents said it was the best solution to locate ballot boxes at easily reachable places such as school gardens or schools that have elevators. Four respondents said special public transportation should be available during elections, while four respondents wanted election officers to visit the houses of those who cannot leave their houses due to a disability or age.

It is logical to claim that increasing the accessibility of ballot boxes should be the first priority for the administration. In fact, there is a prime ministerial circular order that aims to make all public buildings and transportation vehicles accessible to disabled citizens by the year 2012 (R.G. no: 26226, 12.07.2006)[7]. However, this is a valid proposal only for those who can actually leave their houses and not for those who must stay at home. Furthermore, uneven distribution of the disabled voters among neighborhoods, districts or villages makes it hard to allocate special ballot boxes at every voting area, too. Appointing teams of election officers to visit the disabled voters at home seems to suffer from the same disadvantages due to geographical dispersion. Thus, increasing the accessibility for those who can manage to reach the voting area and legalizing proxy voting for heavily disabled citizens can be considered primary solutions. However, surprisingly, it is important to note that none of the respondents favored proxy voting as an alternative. Clearly the respondents were keen on voting in person rather than trusting someone else, as they could never be completely sure of their vote.

After highlighting some drawbacks of possible solutions, we may ask whether mobile voting could be a viable option for them. The answer to this question depends on the attitudes of the voters and the governments. On the government side, the main problems are said to be identification and privacy issues. Yet, it could be claimed that the enthusiasm of the state for e-government applications makes electronic voting one of the possible methods of voting. In 2003, electronic voting was added to the electoral law as a method of voting along with postal voting, although it is only for the citizens who live abroad. Additionally, it could be claimed that Turkey has accumulated enough experience in e-government services to overcome any identification and privacy issues. Turkey, as a candidate for the European Union (EU), and as a partner involved in e-government agenda of the union, has been eager to invest in e-government projects since the 1990s with programs like E-Turkey and E-Transformation Turkey. In 2010, Turkey's rate of providing twenty e-government services, as determined by the EU, was 88,75%, above the average of the other twenty-seven countries (84,28%). Some of the services offered via the e-government portal (www.turkiye.gov.tr) are also accessible through mobile phones. Legal basis of electronic signature and mobile signature have already been established, and they are used for formal transactions in areas like banking and commerce. Thus, it is possible to claim that mobile voting is not out of reach from a technical point of view.

[7] Unfortunately, it seems the architectural accessibility remains a problem as of 2012 due to lack of resources.

On the other hand, mobile voting is not all about technical feasibility. People may simply not like the idea of voting through a mobile phone, in which case an immature initiative may end up in disappointment. It is this aspect of the problem that this paper aims to focus on hereafter. In order to investigate disabled voters' opinions about mobile voting, a questionnaire was e-mailed to disabled voters who are either members of the forum or members of disability associations. The questionnaire involved 16 expressions, which aimed to investigate the opinions of respondents about whether they believed the necessary social, and technologic substructure for mobile voting existed in Turkey, as well as expressions about the opinions on the fairness and secrecy of mobile voting. The respondents were asked to choose one of five options (Totally Agree, Agree, Undecided, Disagree, Absolutely Disagree) about the expressions. Table 1 shows the properties of the respondents, while Table 2 shows the frequencies of the answers for each of the expressions.

		Frequency	Percent	Valid Percent	Cumulative Percent
Age	20-29	9	22,5	22,5	22,5
	30-39	19	47,5	47,5	70,0
	40-49	9	22,5	22,5	92,5
	50+	3	7,5	7,5	100,0
	Total	40	100,0	100,0	
Gender	Female	17	42,5	42,5	42,5
	Male	23	57,5	57,5	100,0
	Total	40	100,0	100,0	
Disability Ratio(%)	-25	1	2,5	2,5	2,5
	26-50	8	20,0	20,0	22,5
	51-75	19	47,5	47,5	70,0
	76-90	5	12,5	12,5	82,5
	91+	7	17,5	17,5	100,0
	Total	40	100,0	100,0	

Table 2: Properties of the Respondents

	Absolutely Disagree	Disagree	No opinion	Agree	Totally Agree
I have to overcome numerous obstacles at elections.	10,0%	2,5%	2,5%	32,5%	52,5%
I believe there is adequate technologic infrastructure for SMS voting in Turkey.	17,5%	12,5%	17,5%	27,5%	25,0%
SMS voting is not appropriate since it would imprison disabled voters at home at the election day.	22,5%	42,5%	12,5%	12,5%	10,0%
Turkish society is ready for SMS voting.	20,0%	25,0%	12,5%	25,0%	17,5%
SMS voting is not appropriate since the voter would be open to external pressures.	17,5%	32,5%	17,5%	12,5%	20,0%
Voter turnout would be higher if SMS voting were possible.	2,5%	5,0%	10,0%	40,0%	42,5%
I do not think SMS voting is appropriate since I do not believe the votes will remain secret.	15,0%	30,0%	15,0%	25,0%	15,0%
SMS voting is not appropriate because of security reasons (viruses, hackers etc.).	17,5%	25,0%	27,5%	15,0%	15,0%
Whatever the technology, it would not compensate sealing the stamp on a paper.	35,0%	37,5%	10,0%	7,5%	10,0%
My family or my friends would interfere if SMS voting from home were possible.	40,0%	37,5%	2,5%	15,0%	5,0%
I could pay a reasonable fee if SMS voting were possible.	25,0%	22,5%	5,0%	27,5%	20,0%
SMS voting is unfavorable since mobile phone operators may manipulate votes.	15,0%	17,5%	17,5%	25,0%	25,0%
I could easily use my mobile phone if SMS voting were possible.	2,5%	12,5%	7,5%	17,5%	60,0%
I do not want to vote whatever the technology since the votes do not change anything.	57,5%	15,0%	7,5%	7,5%	12,5%
I would prefer to vote by fixed phone, mail or fixed computers rather than mobile phones.	12,5%	22,5%	30,0%	17,5%	17,5%

Table 3: Frequencies of the Answers for the Expressions (%) (N:40)

Although these results are not suitable for making generalizations, they may be used to illustrate risks and opportunities for mobile voting in Turkey. To start with, it is evident that the respondents are eager to use their voting rights, and they believe their votes count. 72.5% of the respondents reject the idea that they would not vote even if mobile voting were possible since they did not believe their votes would change anything. However, a great majority of the respondents (85%) say that they have to overcome many obstacles to exercise their voting rights on election day. At this point, the answers of the respondents provide clues as to whether mobile voting would alleviate problems for them and other voters. More than half of them (52,5%) believe technologic infrastructure for mobile voting is adequate and a large majority (82,5%) think that voter turnout would increase if mobile voting were possible, and 77,5% of them say they can easily use mobile phones for voting if SMS voting were possible. In addition to that, 77,5% percent of the respondents reject the idea that their families or friends would interfere or try to affect their votes, which may be regarded as one of the greatest risks associated with mobile voting.

However, mobile voting is not without problems. The respondents have suspicions about the freeness, fairness, and anonymity of mobile voting, interestingly enough, not because of the technology itself but because of negative impressions about society and corporations. 50% of the respondents agree that SMS voting is inappropriate because mobile phone operators would manipulate votes, which is a higher percent than those who are suspicious due to viruses or hackers (30%). Thus, it could be claimed that an immature implementation of mobile voting may be open to trust attacks, which is a greater risk as trust among citizens are already problematic.

Summing it up, it is possible to claim that the technological infrastructure in Turkey is developed enough to support mobile voting for those who need it to gain real access to polling stations. This would bypass many of the legal, architectural, and practical problems that are faced on election day. The respondents' answers show that disabled voters can easily use this technology. Mobile phones have a wide range of accessibility options when it comes to accommodating disabilities. In addition, respondents' answers cast general doubt on what many view as a disadvantageous aspect of e-voting: suspicions about the secrecy of the votes. Most of them do not think their family members or friends would interfere if mobile voting were possible. It is also true that there are trust issues that need to be solved. For those who cannot trust new voting types, mobile voting could simply be an option. However, the most important trust issue seems to be about the political culture and the role of private sector.

5 Conclusion

As a burgeoning technology, mobile voting is, like any youngster, full of potential rather than accomplishments. The foremost consideration about mobile voting seems to be trust issues, not about the technology itself but rather the democratic culture of the country. If voters do not trust other citizens, their governments, or private corporations, they would refuse to use any innovation, no matter how new technology could simplify things for them.

It could be argued that a significant proportion of the disabled voters in Turkey have to overcome many obstacles on election day to make their voices heard. Although there are legal regulations to make things easier for them, real life experiences make them feel left out. There are a number of alternatives for disabled voters. Proxy voting and increasing accessibility of the ballot boxes seem to be primary options that could be achieved in a short time. Mobile voting by SMS or other such devices may be considered a strong alternative for disabled voters in Turkey too. The legal and technological basis of such an endeavor already exists in Turkey. However, trust building should be a primary task, and a long-term agenda should be set to prepare the society for new voting types (esp. about public-private partnership, establishing clear security protocols, and extensive PR activities). In this process, pivotal work could be designed to target social groups such as disabled voters or young voters, groups which may be more enthusiastic about mobile/electronic voting or which need these innovations to their rights as citizens.

Bibliography

[Bo00] BOON; M. et.al.: Local Elections Pilot Schemes 2007 (Report for The Electoral Commission of UK), www.electoralcommision.org.uk, 2007

[BB03] BRÜCHER, H.; BAUMBERGER, P.: "Using Mobile Technology to Support eDemocracy", hicss,pp.144b, 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 5, 2003.

[Ca06] CASTELLS, M. (2006); Mobile Communication and Society: A Global Perspective, Cambridge, MA, USA: MIT Press, 2006.

[Ge04] GESER, H.: "Towards a Sociology of the Mobile Phone", in Sociology in Switzerland: Sociology of the Mobile Phone, Online Publications. Zurich, May 2004 (Release 3.0), http://socio.ch/mobile/t_geser1.pdf , accessed 15.02.2009.

[GC00] GRAY, M.; CAUL, M.: "Declining Voter Turnout in Advanced Industrial Democracies, 1950 to 1997", Comparative Political Studies, Vol. 33, No. 9, 1091-1122, 2000.

[Jo02] JONES, N.: SMS Voting Is a First Step Toward Mobile Democracy, Research Note, Gartner, 2002.

[KK04] KUSCHU, İ.; KUŞÇU, M. H.: “From E-Government to M-Government: Facing the Inevitable?”, in Proceedings of 3rd European Conference on e-Government, Frank Bannister and Dan Remenyi (eds.), 3-4 July 2003, Trinity College, Dublin Ireland, http://www.mgovernment.org/resurces/mgovlab_ikhk.pdf (mGovLab.org copy), 2004.

[Lo02] Local Governments Association (LGA): The Implementation of Electronic Voting in UK (research summary), LGA Publications, London, www.electoralcommision.org.uk, 2000.

[MB01] MAIR, P.; van BIEZEN, I.: “Party Membership in Twenty European Democracies 1980-2000”, Party Politics, vol:7, no:1, 5-21, 2001.

[Mo03] MORI: Public Opinion and the 2003 Electoral Pilot Schemes (Research Study for The Electoral Commission), www.electoralcommision.org, 2003..

[Ny05] NYIRI, K.: “The Mobile phone in 2005: Where Are We Now?”, Seeing, Understanding, Learning in the Mobile Age Presidential Address, 28-30 April 2005, Budapest, http://www.fil.hu/mobil/2005/, accessed 15.02.2009.

[Sc03] SCARROW, E. et.al.: “New Forms of Democracy? Reform and Transformation of Democratic Institutions”, in (CAIN, Bruce; DALTON, Russel J.; SCARROW, E. Susan Eds.): Democracy Transformed?, Oxford University Press, London, 2003, pp. 1-20.

[Sr05] SRIVASTAVA, L.: “Dissemination and Acquisition of Knowledge in the Mobile Age”, Seeing, Understanding, Learning in the Mobile Age Conference Opening Speech, 28-30 April 2005, Budapest, http://www.fil.hu/mobil/2005/, accessed 15.02.2009.

[Su06] SUÁREZ; S. L.: “Mobile Democracy: Text Messages, Voter Turnout And The 2004 Spanish General Election”, Representation, 42:2,pp. 117-128, 2006.

A New Implementation of a Dual (Paper and Cryptographic) Voting System

Jonathan Ben-Nun[1], Niko Farhi[1], Morgan Llewellyn[2], Ben Riva[1], Alon Rosen[3], Amnon Ta-Shma[1], Douglas Wikström[4]

[1]Tel Aviv University
Israel
jonathan.bennun@gmail.com
{nikofarh | benriva | amnon@tau.ac.il}

[2]IMT Lucca
Italy
morgan.llewellyn@imtlucca.it

[3]IDC Herzliya
Israel
alon.rosen@idc.ac.il

[4]KTH Stockholm
Sweden
dog@csc.kth.se

Abstract: We report on the design and implementation of a new cryptographic voting system, designed to retain the "look and feel" of standard, paper-based voting used in our country Israel while enhancing security with end-to-end verifiability guaranteed by cryptographic voting. Our system is dual ballot and runs two voting processes in parallel: one is electronic while the other is paper-based and similar to the traditional process used in Israel. Consistency between the two processes is enforced by means of a new, specially-tailored paper ballot format. We examined the practicality and usability of our protocol through implementation and field testing in two elections: the first being a student council election with over 2000 voters, the second a political party's election for choosing their leader. We present our findings, some of which were extracted from a survey we conducted during the first election. Overall, voters trusted the system and found it comfortable to use.

1 Introduction

The foundations of modern cryptographic voting systems were laid out in the 1990s, introducing powerful techniques such as homomorphic tallying and mixing networks. Almost all early work assumes that the voter has access to some trusted computational device while voting. In 2004, Chaum [Ch04] and, independently, Neff [Ne04] proposed

cryptographically secure voting systems in which the voter has access to no computational device at the time of voting. Since then, most research has focused on such bare-handed, end-to-end verifiable voting systems.

In 2008, Benaloh [Be08] suggested dual voting. In Benaloh's system, the voter fills in a plaintext ballot and a scanning machine reads it to produce a printed plaintext ballot, which is cast into a ballot box, together with a cryptographic encryption, which is uploaded to a public web page, and an electronic receipt, which the voter may take home. The system is end-to-end verifiable using standard cut-and-choose techniques.[1]

There are several advantages to dual voting. Cryptographic voting, in general, is more vulnerable than paper-based voting to global failures and attacks. We can demonstrate this with a simple global failure. Many cryptographic protocols use a k-out-of-n threshold encryption scheme. It may happen that (accidently or deliberately) too many keys are lost, in which case the whole election is compromised. Paper-based systems are, in contrast, more resistant to global failures. Thus, dual-voting systems supply the stronger guarantees of end-to-end verifiability characteristic of electronic cryptographic voting while retaining paper's resiliency against global failures.

Another major advantage of dual voting is psychological. Dual-voting systems often retain the look and feel of paper-based systems, which makes these systems more familiar to and trusted by voters, who are used to paper-based voting. Furthermore, we saw time and again that people trust paper, probably because paper is something you can hold and read on your own. The fact that our system offers a paper backup made it easier for the Merez party to decide to use our system.

In dual-ballot systems, an adversary wishing to commit election fraud would need to break both the paper-based and the cryptographic systems.[2] On the downside, it is enough to break one system to breach privacy.

Finally, it should be noted that in dual-ballot systems it must be decided in advance when to count which system. Indeed, in some states (like California) the law requires to count paper ballots, while in others, only a sample is required. We find the following options reasonable:

- Use the paper-based system as backup only for disaster recovery, e.g., when private keys are lost or when the bulletin board goes down during the election.
- Count both systems (for all polling stations or for a sample of them) and if they substantially differ, conduct an official investigation.

---

[1] In fact, Benaloh's system may be seen as a triple voting system, where the scanner tallies the scanned votes in addition to the electronic and paper tallying.

[2] In most cryptographic systems the integrity guarantee is unconditional, even against all-powerful adversaries, and so it is often heard that cryptographic systems cannot be undetectably forged. However, it should be noted that the cryptographic guarantee is given only provided certain assumptions hold, e.g., the authenticity of the bulletin board is assumed.

While the theory of cryptographic voting is extensive, and quite well understood, not many cryptographic voting systems have been tested in practice. Helios [Ad08, Ad09], which is a web-based voting system, has been used in several elections totaling more than 25,000 voters. Prêt-a-Voter was tested at the University of Surrey Student Union elections in 2007 [Bi09]. We mention that a recent version of Prêt-a-Voter [LR08] also supports dual voting. Punchscan was used at the University of Ottawa in 2007 [EC07]. Scantegrity II was used at the Takoma Park, Maryland municipal elections in 2009, serving over 1,700 voters [Ca10]. Scantegrity II also supports dual-voting. With the exception of Helios, all the other systems use pre-prepared ballots.
A common criticism of cryptographic voting systems concerns the usability issue. It is often said that cryptographic voting systems are too complicated for the common voter. In this work we set to design and implement a dual ballot system that retains the look and feel of paper-based elections in our country, trying to prove that such systems do not suffer from usability issues. We implemented a bare-handed, end-to-end verifiable, dual (paper and electronic) system with ballots printed on-demand (as opposed to pre-prepared ballots). Our design is closest to Benaloh's system [Be08] and has been adapted to Israel's paper-based system.

Our system was successfully tested twice. It was first used in an the Interdisciplinary Center's student council election held in May 2011 and then again in Merez's party leader election held in February 2012. We summarize our experience as follows:

> **IDC's Election:** The Interdisciplinary Center (IDC) is a non-profit college with around 6,000 registered students; 2,097 students voted in the election. We counted both the electronic and paper-based systems and discovered minor differences between the two tallies, most likely attributed to mistakes in the hand-counted paper tally. 481 voters checked their receipts online.3 We had only two complaints about missing receipts, which we attribute to scanning errors.
> We also asked voters to fill in a questionnaire about the voting experience, asking about their understanding of the voting process and their satisfaction from it. The results show that the majority of survey respondents thought the voting process was clear and simple and possessed a high degree of confidence in their vote being counted. We report on the survey results in Section 4.2. It should be kept in mind, though, that most of the voters were young and often technologically savvy students.
>
> **Merez's election:** Merez is a small political party in Israel and has about 3% of the seats in parliament. The party council, with about 950 representatives, elects the party's leader. There was a high turnout at the elections with approximately 830 voters (88% of registered voters). Many of the voters were over 50 years old. Due to limited resources, we did not run a questionnaire at the election, but we received enthusiastic feedback from many voters and officials, with the party's secretary-general saying over 60 representatives called him to say how good it was to use our voting system.

[3] We gave the voters an incentive to verify their vote online.

We believe the fact that our system retains the look and feel of current paper-based voting systems helped people accept it and made them think of the dangers and promises of electronic voting. We hope that our experiment will help facilitate the transition from paper-based voting to more sophisticated systems supporting end-to-end verifiability.

2 Desired Properties

The most crucial property required of electronic voting systems is *integrity*, meaning that it is impossible to falsify election results. Another crucial property is *privacy,* meaning that no one can link a voter to his or her vote, and even further, a voter cannot prove to someone, what his or her vote was. Such a system is known as *coercion-free* or *incoercible* and helps reduce the chances of vote buying.

A system is *voter-verifiable* if any voter can verify that his/her vote was correctly recorded and is included in the tally. A system is universally-verifiable if *anyone* can verify that all recorded votes are properly tallied. A system having both properties is *end-to-end* verifiable.

One can roughly divide the new voting systems into two classes: voting systems where ballots are pre-prepared before election day [Ch04,RP05,FCS06,AR06,Chb08,Cha08] and voting systems where ballots are printed on-demand in the voting booth behind curtains [Ne04,MN06,Be06,Be08, SDW08]. On-demand systems often have easy, user-friendly interface for the voter (often using touch screens). Regarding privacy, with print-on-demand voting the voter often has to enter his or her choices into the voting machine - thus losing privacy with respect to the voting machine, whereas pre-prepared ballots avoid this problem. On the other hand, when ballots are printed in advance it is crucial to guarantee that these ballots are kept secret (for instance, that the ballots are not photocopied by an adversary) leading to the *chain of custody* problem. Another privacy issue in print-on-demand systems is the possibility of subliminal channels where the booth leaks information about the votes to outsiders. For example, the booth can pick randomness that would create a ciphertext whose last bits would also encode the candidate. [FB09,AN09,GGR09] These resources show how to mitigate these types of attacks.

3 The Protocol

Our protocol is based on the protocols from Benaloh [Be06, Be08]. Since the voting booth in our protocol prints ballots on-demand, we protect against subliminal channels by splitting some of the booth's functionality to external smart cards (see Appendix A for further details.)

Our system uses standard cryptographic primitives used in other cryptographic voting protocols. More specifically, we use the following protocols: ElGamal encryption scheme [Ga85]; Pedersen's (t, n) -threshold ElGamal encryption scheme[Pe91, Pe92], in which any t parties can decrypt a message but no $t-1$ parties can; Cramer et al.'s three round, honest-verifier zero-knowledge proof system [CDS94], proving an ElGamal ciphertext c is an encryption of a message m from a given set of possibilities $m_1, \ldots, m_l$; the Fiat-Shamir heuristic to transform public-coin, zero-knowledge proofs to non-interactive ones; and we use a *universally verifiable* mix-net producing non-interactive, zero-knowledge correctness proofs. We chose to use a mix-net rather than homomorphic tallying because mix-nets support a wider range of voting schemes.

3.1 Trust Model

Assumptions assuring integrity: We assume the polling station workers are semi-honest, i.e., they will not allow someone to upload encrypted votes or to cast plaintext votes that were not legitimately cast by voters.

Assumptions assuring incoercibility (and privacy): We assume the voting booth will remain integrous, not collaborating with any coercer or with any of the smart cards it uses. We further assume that the smart cards are manufactured by different companies and are not able to collaborate amongst themselves. We also assume that the smart cards can be initialized only once and their internal memory cannot be read or modified externally. Last, we assume there is no dishonest subset of the mix-net parties large enough to be able to decrypt messages.

3.2 High-level Description

The voter first enters the polling station and identifies herself to the polling station committee. Once cleared, the voter proceeds to the voting booth and makes her selection on a touch screen. The voting machine then prints a *dual-ballot*. At this point in the process the voter can either audit the machine, or, use the ballot for casting (i.e., we employ Benaloh's [Be06] *cast-or-audit* method).

Our dual-ballot is a paper note, divided into two detachable parts: the electronic ballot and the physical (*plaintext*) ballot (see Figure 1). The electronic ballot contains the encrypted vote along with a digital signature certifying the electronic ballot. The physical ballot shows the actual vote printed on it. It can be folded in half and then sealed using a standard adhesive, thereby hiding the plaintext inside.

If the voter intends to cast the ballot, the voting machine prints ”For Casting” on the ballot (see Figure 1). The voter then folds and seals the physical ballot (see Figure 3) and exits the voting booth. The electronic ballot is scanned by the polling station committee and the information is uploaded to the public electronic bulletin board. The committee stamps both parts of the ballot and detaches them in front of the voter. The physical ballot is cast into the ballot box and the electronic ballot is taken home by the voter as a receipt (see Figure 4).

If the voter intends to audit the ballot, the voting machine prints additional audit information on the ballot (see Figure 2). Audit ballots allow one to check the consistency of the voting machine, and inconsistent audit ballots serve as a proof that a given voting machine does not function correctly. Audit ballots cannot be used for voting; to cast an actual vote, the voter must re-enter the voting booth.

Tallying: Once the polling stations close, the electronic tallying process takes place publicly on the bulletin board. The tallying is performed using cryptographic tools, such as mix-nets and zero-knowledge proofs. Manual tallying of the paper ballots may be performed at the polling station once it is closed. The decision whether to count/sample the paper ballots or not is left to the discretion of the officials organizing the elections. A policy defining when paper ballots will be tallied should be published prior to the elections.

A detailed description of the protocol appears in Appendix A.

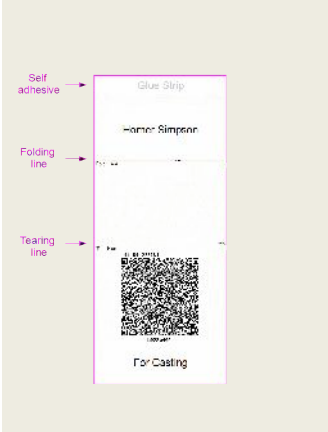


Fig. 1: Dual-ballot before folding. Since it is for casting, there is no barcode in the lower part of the ballot

Fig. 2: Audit ballot. The audit information is printed in the barcode in the lowest part of the ballot

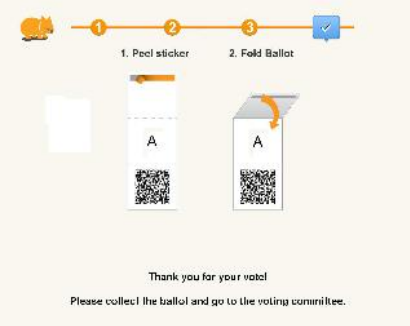


Fig. 3: Folding a ballot

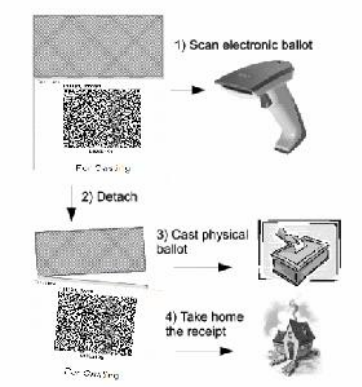


Fig. 4: Casting

3.3 Implementation

According to the protocol, the machine has to commit to the encryption before knowing whether or not the ballot has been audited. To implement this, the printer output slot is protected by a partially transparent plastic cover that lets the voter see the partially-printed ballot without seeing what is printed on it. This also prevents using the cipher-text as a source of randomness for coercion.

An important implementation detail concerns the choice whether to audit the ballot or not. At first, we asked each voter if he or she would like to audit the ballot. We discovered that many voters were confused by that question. As a result we decided to hide the ballot-auditing feature from common voters. Instead, in our implementation the audit option can be invoked by pressing a hidden button while the ballot is printed (see Figure 5). The rationale behind this is the fact that it is sufficient to audit approximately 2-3% of the ballots, and this can be done by designated auditors. That way, we simplify the voting experience for the common voter without sacrificing the security of the system.

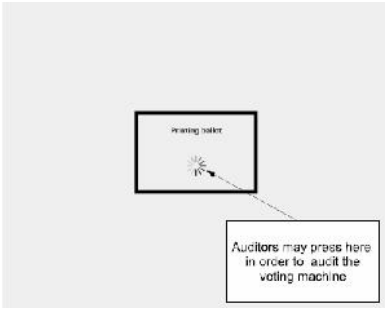


Fig. 5: Screenshots of the printing window with the hidden audit button

We advertised this procedure on the web page so that more sophisticated voters could also participate in the auditing process.

Our website displayed encrypted votes and some additional information about the election like explanations about the voting, auditing and tallying processes, all public keys, the mix-net proofs of correctness, the uploaded votes file and signature, and election results. Voters can also use the website to find their votes inside the vote file.
For the mix-net, we use Verificatum [Ve11], which is a free and open source implementation of an ElGamal based mix-net. Most of the code is written in Java, but arithmetic code is also available for improved speed. For more details about the protocol itself we refer the reader to Wikström [Wi11]. We are currently in the final stages of writing an independent verifier for the proofs generated by Verificatum.
We also wrote an open source Android application allowing voters to audit their votes more easily. The application allows voters to take a picture of the ciphertext part of the

ballot and the audit part of the ballot (if it exists) using the smart phone's camera. The application verifies that the signatures on the ballot are correct. If the ballot is an audit ballot, the app would ensure that the ciphertext was generated using the randomness specified in the audit part. If it is "For Casting", the app verifies the ciphertext information is posted correctly on the website.

3.4 Unimplemented Functionality

The protocol uses smart cards to mitigate a subliminal channel attack. However, we had neither the time nor the resources to build and test a system with smart cards. Instead, we simulated the smart card functionality. We hope to add actual smart cards in later versions of the system.

In our original design, the polling stations would only upload the new votes to the website. To make sure the website would not remove chunks of votes from the list, the posted votes were to be protected by Merkle Hash Tree [Me87]. However, due to time restrictions, and the fact that we supported only one polling station, we decided to upload all votes to the website.

4 Usability and Related Issues

The IDC elections took place for three consecutive days, from May 17th to 19th. There were several simultaneous races: In addition to races for the student council president, vice president, and elections for representatives of 27 special tracks, 78 candidates competed for 56 available seats on the student council. About 2,097 voted in the election out of about 6000 registered voters (approximately 33%). Most of the voters were students in their early 20s. On average, it took a voter 1-2 minutes to vote, comprised of about 30 seconds of interacting with the polling station worker before voting, one minute using the voting machine, and another 30 seconds of interaction with polling station workers after voting. Once polling stations close, the mix-net was run on a single machine. The whole process took slightly less than 20 minutes and the election results were announced 45 minutes after the closing of the polling station on the last day of the elections. No contentions were filed.

In order to educate potential voters about the system, in both elections the voting process was explained in advance on a website. Furthermore, one of the developers stood at the entrance of the polling station and explained the polling process, defining exactly what they had to do once inside the polling station. We also made large posters clarifying the process and posted them outside the polling station.

4.1 Lessons learned

Many voters (in both elections) did not fold their ballots at all or folded them incorrectly, without explicitly being told the proper technique. This was partly due to an insufficient ballot design, which made it possible to fold the ballot in two different ways. When one of the system developers demonstrated the proper folding method for voters before entering the voting booth, the error rate virtually dropped to zero.

We also explained the dangers of DRE voting, i.e., where a computer simply stores the votes internally, to interested voters. Voters quickly understood the issue and many of them told us they feel better knowing they can actually *see* their vote in plaintext. Many voters (especially the younger ones) enjoyed voting with the new technology, and as a result, were more open-minded to learn about the system. Since the usability of electronic voting also depends on the voters' enthusiasm and understanding, we believe these two reactions are positive if one considers large-scale deployment of the system.

4.2 The Questionnaire

In the first election, we asked voters to fill in an on-line questionnaire. (We did not have a questionnaire in the second election because of limited resources.) The online questionnaire was composed of 10 questions: two administrative, six about the voter's understanding of the voting process and his or her satisfaction, and two about the perceived privacy and integrity of the system. In addition, we also conducted random exit surveys. In total, 481 voters participated in the survey, 403 of them answering the on-line survey and 78 the exit survey. The survey response rate was just under 23.4%. About 37% of those who answered were female and 62% were male, with 4 voters declining to state their gender. In general, survey participants were well -distributed among seven fields of study. The majority (about 73 %) of survey participants verified their ballots.

Information on a voter's satisfaction with the voting process was captured via the survey question: "Thinking about your overall experience at the polls today, how satisfied are you with your voting experience?" Responses to this question are posted in Table 1. Over 85% of respondents reported being satisfied.

	Very satisfied	*Satisfied*	*Somewhat dissatisfied*	*Very dissatisfied*	*Don't know*
On-line survey	45.2%	49.6%	2.2%	1.0%	2.0%
Exit survey	62.9%	34.6%	0.0%	2.5%	0.0%

Table 1: Voter Satisfaction

[4] The high participation rate is due to a lottery of two campus parking lots (a desirable bonus) among those who participated.

Voter opinion over the simplicity of the voting process is located in Table 2. The majority of survey respondents believed the voting process was clear and simple. Across all survey participants, 60% of respondents strongly agreed that the voting process was clear and simple; with just over 1% of respondents strongly disagreeing. About three-quarters of survey respondents reported understanding why the ballot was separated.

	Strongly Agree	Agree Somewhat	Neither Agree nor Disagree	Disagree Somewhat	Strongly Disagree
Did not verify	68.5%	20.8%	8.4%	1.5%	0.8%
Verified ballot	56.1%	29.6%	8.9%	4.0%	1.4%

Table 2: The Voting Process Was Clear and Simple

Given that many voters viewed the process as rather straightforward, it is not surprising that voters possessed a high degree of confidence in their votes being counted. Relative to previous studies of voter confidence in U.S. elections, voter confidence was extremely high with 95.1% of voters expressing a high level of confidence [AHL08].

Despite high levels of voter satisfaction, the survey did highlight two areas for future improvement. Approximately 15% of respondents reported encountering a problem or asking for assistance during the voting process. Through a follow-up question, respondents identified folding the ballot as the most commonly encountered difficulty (36% of identified problems). At 14% of the reported problems, the second most cited difficulty was the online verification process. Participants were asked to state the one task which they would like to improve. Out of a list of 9 fixed choices, and one write-in option, 33% of survey respondents selected verifying their ballot on the Internet. These issues are currently being addressed by the design team, and we anticipate future versions of the system to encounter significantly fewer user issues.

In conclusion, voters exhibited high levels of satisfaction and confidence with the system. A clear majority of voters found the voting process simple and uncomplicated which is particularly important when implementing a new e-voting system. Given the unfamiliarity of the concept of vote verification, it is reassuring that most voters were confident and comfortable with the technology. Finally, survey and observational analysis revealed a significant portion of voters encountered problems with the ballot design, especially the folding, which clearly needs to be improved.

Appendix A: Detailed Description of the Protocol

A.1. Setting up the election

The mix-net parties jointly generate a master public key using the distributed key generation of the threshold ElGamal cryptosystem. Let G, q, g be the public parameters and let h be the generated threshold ElGamal public key.

The bulletin board and all polling station committee computers generate signature key pairs. We assume that the bulletin board public key is known to all participants.

Last, the election officials initialize two smart cards SC_1, SC_2 for each voting booth. The initialization of smart card SC_i consists of the generation of a unique identification number id_i and the generation of a signature key pair (possibly the same for all booths) and setting the internal counter $rnd_{cnt_i} = 1$. Also, the election public-key is stored on the card along with the list of valid candidates. All the smart cards' public keys are stored on the bulletin board.

A.2. Election day

Voting: The voter enters the polling station and identifies herself. Once cleared by the poll workers, the voter enters the voting booth. The voter votes v using a touch screen.

Denote the smart cards by SC_1, SC_2. The booth itself is a deterministic machine that cannot generate randomness. The booth requests randomness from the smart cards (to avoid the subliminal channel problem). Each smart card $i \in \{1,2\}$ increases its internal counter by one rnd_{cnt_i} and returns a message consisting of $[rnd_{cnt_i}, r_i, g^{r_i}, Signature_{SC_i}(id_i|rnd_{cnt_i}|g^{r_i})]$ where g is the generator from the election public key and r_i is uniformly random.

The booth encrypts the vote by $c = Enc_h(v, r_1 + r_2)$. It also generates a non-interactive zero-knowledge proof π_c that c is an encryption of a valid vote (using 1-out-of-l zero-knowledge proof). The booth sends $[rnd_{cnt_1}, rnd_{cnt_2}, c, \pi_c]$ to SC_1 (SC_1 is chosen before the election day, e.g. the smart card with lower ID number). The smart card verifies that the proof π_c is valid for c, and that its internal counter sig_{cnt_1} is smaller than rnd_{cnt_1}. If everything is sufficiently verified, the smart card sets its internal counter to $sig_{cnt_1} = rnd_{cnt_1}$ and returns $[Signature_{SC_1}(id_1|rnd_{cnt_1}|rnd_{cnt_2}|c)]$. Otherwise it will display an error message. (We need the 1-out-of-l zero-knowledge proof to prevent the voting machine from leaking previous votes in the encrypted message, thereby violating voter privacy.)

The booth prints the first and second parts of the ballot (see Figure 1). More specifically, in the physical ballot part it prints v and in the electronic ballot it prints:

$$id_1, id_2$$
$$rnd_{cnt_1}, rnd_{cnt_2}$$
$$g^{r_1}, Signature_{SC_1}(id_1|rnd_{cnt_1}|g^{r_1})$$
$$g^{r_2}, Signature_{SC_2}(id_2|rnd_{cnt_2}|g^{r_2})$$
$$c = Enc_h(v, r_1 + r_2), Signature_{SC_1}(id_1|rnd_{cnt_1}|rnd_{cnt_2}|c)$$

The counters are used to prevent chain voting and a re-use of randomness.

We shielded the printer output such that the voter could see that a ballot had been printed but it cannot be extracted before the voter chooses whether or not to audit the ballot.
We note that by using the information printed in the electronic ballot, anyone can verify that the encryption was computed with randomness that was produced by the smart cards. That can be checked simply by verifying all signatures and computing $g^{r_1}g^{r_2}$ and comparing it with the first element $Enc_h(v, r_1 + r_2)$.
Now, the voter can (but does not have to) audit the voting machine to verify that the ballot was produced properly. If the voter wishes check it, she presses "Audit the Machine" on the touch screen. Otherwise, the voter presses "Cast".

Auditing the machine: The booth prints "Audit information: r_1, r_2" at the bottom of the ballot. After the voter exits the booth, the poll-workers verify that all signatures are valid and that the randomness counters are equal and increased by one over the counters of previously casted ballots. By using the randomness printed as audit information the poll workers can verify that the ciphertext printed on the electronic part of the ballot really encrypts the plaintext printed on the other part. If so, they stamp the ballot and the voter can return to the booth to continue her voting. The voter may also verify those properties at home.

Casting: If the voter presses "Cast" the booth prints "For Casting" at the bottom of the ballot. The voter folds the first part of the ballot. Next, the voter leaves the voting booth and presents her folded ballot to the poll workers. The poll workers verify that her ballot has not yet been detached. They scan the electronic ballot, verify its signatures and randomness counters, stamp both parts of the ballot, and detach the physical ballot from the electronic one. All of this is done in front of the voter. The physical ballot is publicly put into the ballot box and the stamped electronic part is uploaded to the bulletin board and returned to the voter as receipt.
The voter then leaves the polling station with the electronic ballot.

A.3. Tallying

After the election is over, the mix-net at every polling station takes all the encrypted votes $c_1, c_2, \ldots, c_N$ and passes them through a (re-encryption) mix-net. The mix-net is made of n mixes, each one belongs to a different party. After the last mix outputs a list of ciphertexts, $c'_1, c'_2, \ldots, c'_N$, a verifiable threshold decryption is executed by t parties. The result of this decryption is the tally result for this specific polling station.
The physical ballots may also be counted according to the policy of the officials organizing the elections.

A.4. Auditing

Auditability of casting: The voter can check whether her casted electronic vote is posted correctly on the bulletin board. Also, she can choose to audit the voting machine and receive an audit ballot that she can check at her home, using her own computer. Because the machine has to commit to the ballot by printing it before it knows whether it is audited or not, the machine has to decide whether to "cheat" or not before knowing whether the ballot will be audited.

Auditability of tallying: Universal verifiability of the tallying is achieved using the standard primitives of verifiable shuffles and verifiable threshold decryption. Anyone can download a program to check those proofs using his or her own computer. Anyone with sufficient knowledge can write a program to verify those proofs themselves.

Cross checking: At the end of the election we get two parallel systems that can validate each other. The decision whether or not to count the paper-based system should be determined before the election takes place.

Bibliography

[Ad08] Ben Adida. Helios: web-based open-audit voting. In USENIX Security Symposium, 2008.

[Ad09] Ben Adida, Olivier Pereira, Olivier DeMarneffe, and Jean jacques Quisquater. Electing a university president using open-audit voting: Analysis of real-world use of Helios. In EVT/WOTE, 2009.

[AHL08] R.Michael Alvarez, Thad E. Hall, andMorgan H. Llewellyn. Are Americans Confident Their Ballots Are Counted? The Journal of Politics, 70(03):754–766, 2008.

[AN09] Ben Adida and C. Andrew Neff. Efficient receipt-free ballot casting resistant to covert channels. In EVT, 2009.

[AR06] Ben Adida and Ronald L. Rivest. Scratch and Vote: Self-Contained Paper-Based Cryptographic Voting. In WPES, 2006.

[Be06] Josh Benaloh. Simple verifiable elections. In EVT, 2006.

[Be08] Josh Benaloh. Administrative and Public Verifiability: Can We Have Both? In EVT, 2008.

[Bi09] David Bismark, James Heather, RogerM. A. Peel, Steve Schneider, Zhe Xia, and Peter Y. A. Ryan. Experiences Gained from the first Pret A Voter Implementation. REVOTE, 2009.

[Ca10] Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, and Poorvi L. Vora. Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy. In USENIX conference on Security, 2010.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In CRYPTO, 1994.

[Ch04] David Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. IEEE Security & Privacy, 2(1):38–47, 2004.

[Cha08] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In EVT, 2008.

[Chb08] David Chaum, Aleks Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan Sherman, and Poorvi Vora. Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting. IEEE Security and Privacy, 6:40–46, 2008.

[EC07] Aleks Essex and Jeremy Clark. Punchscan in practice: an E2E election case study. In WOTE, 2007.

[FB09] Ariel J. Feldman and Josh Benaloh. On subliminal channels in encrypt-on-cast voting systems. In EVT, 2009.

[FCS06] Kevin Fisher, Richard Carback, and Alan T. Sherman. Punchscan: Introduction and system definition of a high-integrity election system. In WOTE, 2006.

[Ga85] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In CRYPTO, 1985.

[GGR09] Ryan W. Gardner, Sujata Garera, and Aviel D. Rubin. Coercion resistant end-to-end voting. In FC, 2009.

[LR08] David Lundin and Peter Y. A. Ryan. Human Readable Paper Verification of Pret a Voter. In ESORICS, 2008.

[Me87] Ralph Merkle. A Digital Signature Based on a Conventional Encryption Function. In CRYPTO. 1987.

[MN06] Tal Moran and Moni Naor. Receipt-Free Universally-Verifiable Voting With Everlasting Privacy. In CRYPTO, 2006.

[Ne04] Andrew Neff. Practical High Certainty Intent Verification for Encrypted Votes. 2004.

[Pe91] Torben P. Pedersen. A Threshold Cryptosystem without a Trusted Party (Extended Abstract). In EUROCRYPT, 1991.

[Pe92] Torben P. Pedersen. Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem. PhD thesis, 1992.

[RP05] Peter Ryan and Thea Peacock. Pret a Voter: a System Perspective. Technical Report 929, University of Newcastle upon Tyne, School of Computing Science, Apr 2005.

[SDW08] Daniel Sandler, Kyle Derr, and Dan S. Wallach. VoteBox: a tamper-evident, verifiable electronic voting system. In USENIX Security Symposium, 2008.

[Ve11] Verificatum project, 2011. http://www.verificatum.org.

[Wi11] Douglas Wikström. Verificatum, 2011. In preparation.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

TECHNISCHE UNIVERSITÄT DARMSTADT

e-voting.cc

Robert Krimmer and Melanie Volkamer (Eds.)

6th International Conference on Electronic Voting

EVOTE2014

28–31 October 2014, Lochau/Bregenz, Austria

Co-organized by

Tallinn University of Technology
Ragnar Nurkse School of Innovation and Governance

Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt

E-Voting.CC GmbH
Competence Center for Electronic Voting and Participation

IEEE
Region 8 (Europe)

Gesellschaft für Informatik
German Informatics Society, SIG SEC/ECOM

PROCEEDINGS

IEEE

German Informatics Society

Robert Krimmer and Melanie Volkamer (Eds.)

6th International Conference on Electronic Voting

EVOTE2014

28–31 October 2014, Lochau/Bregenz, Austria

Co-organized by the Tallinn University of Technology, Technische Universität Darmstadt, E-Voting.CC, IEEE and Gesellschaft für Informatik

TUT PRESS

Proceedings EVOTE2014
TUT Press

ISBN 978-9949-23-685-5 (PDF)
ISBN 978-9949-23-688-6 (publication)

Volume Editors

Prof. Dr. Robert Krimmer
Tallinn University of Technology
Ragnar Nurkse School of Innovation and Governance
Akadeemia tee 3
12618 Tallinn
Estonia
E-mail: robert.krimmer@ttu.ee

Prof. Dr. Melanie Volkamer
Technische Universität Darmstadt
Hochschulstrasse 10
64289 Darmstadt
Germany
E-mail: melanie.volkamer@cased.de

Citation Recommendation: Author (2014): Title. In: Krimmer, R., Volkamer, M.: Proceedings of Electronic Voting 2014 (EVOTE2014), TUT Press, Tallinn, p. xx-yy.

printed by TUT Press, Tallinn

Printed with grateful support from the Austrian Federal Ministry of the Interior.

Preface

In 2004, the first Conference on Electronic Voting took place at Castle Hofen. Since then, the biannual EVOTE conference has become a central meeting place for e-voting researchers with different backgrounds and e-voting practitioners including vendors, observers, and election authorities. This conference is one of the leading international events for e-voting experts from all over the world. Cumulatively, over the years 2004, 2006, 2008, 2010 and 2012 more than 450 experts from over 30 countries have attended this conference to discuss electronic voting topics.

In so doing, they have established Bregenz as a regular forum and point of reference for the scientific community working with e-voting. One of its major objectives is to provide a forum for interdisciplinary and open discussion of all issues relating to electronic voting. The multidisciplinary EVOTE conference celebrate this year its tenth birthday. This year is centered on the theme "Verifying the Vote" and to review what has been accomplished since 2004. We are particularly happy to convince IEEE to publish EVOTE papers as post proceedings with them.

The diversity and multidisciplinary of EVOTE is also reflected in the program committee of EVOTE 2014 and in the 17 papers selected. These 17 papers were selected out of the 33 submissions based on a double blind-review process. 10 of the 17 accepted papers will also be published with IEEE. The program also features three invited talks:

- Yulimar Quintero Trumbo (Election Expert):
  Electoral Technology: Observations across Latin America
- Vanessa Teague (University of Melbourne):
  Trust and Verifiability in Australian E-voting
- Geo Taglione and Oliver Spycher (Swiss Federal Chancellery)
  Internet Voting in Switzerland - Where We Stand Today
-

The accepted papers represent a wide range of technological proposals for different voting settings (be it in polling stations, remote voting or even mobile voting) and case studies from different countries already using electronic voting or having conducted first trial elections.

Special thanks go to the international program committee for their hard work in reviewing, discussing and shepherding papers. They ensured the high quality of these proceedings with their knowledge and experience.

We also would like to thank the German Informatics Society (Gesellschaft für Informatik) with its ECOM working group for their partnership over several years. A big thank you goes also to the Austrian Federal Ministry of the Interior and the Regional State of Voralberg, for their continued support. Further thanks go to the platinum conference sponsor Scytl.

Tallinn, Darmstadt, October 2014 Robert Krimmer, Melanie Volkamer

This conference is co-organized by:

Tallinn University of Technology -
Ragnar Nurkse School of Innovation and Governance

Technische Universität Darmstadt -
Center for Advanced Security Research Darmstadt

E-Voting.CC GmbH -
Competence Center Electronic Voting & Participation

IEEE – Region 8 (Europe)

Gesellschaft für Informatik,
German Informatics Society, SIG SEC/ECOM

Supported by:

Federal Ministry of the Interior - Austria

Regional Government of Vorarlberg

Sponsored by:

Scytl S.A. – Platinum Sponsor

International Programme Committee

Alvarez, Michael Caltech, USA
Araujo, Roberto Universidade Federal do Pará, Brazil
Bannister, Frank Trinity College, Ireland
Barrat, Jordi EVOL2 - -eVoting Legal Lab / University of Catalonia, Spain
Benaloh, Josh Microsoft, USA
Besselar, Peter van den Vrije Universiteit Amsterdam, Netherlands
Beznosov, Konstantin University of British Columbia, Canada
Bismark, David Votato, Sweden
Bock Segaard, Signe Institute for Social Research, Norway
Braun Binder, Nadja Research Institute Public Administration Speyer, Germany
Buchsbaum, Thomas Ministry for European and Internat. Affairs, Austria
Bull, Christian Ministry of Local Government and Modernisation, Norway
Caarls, Susanne Federal Ministry of the Interior, Netherlands
DeGregorio, Paul A-Web, USA
Dittakavi, Chakrapani CIPS, India
Drechsler, Wolfgang Tallinn University of Technology, RNS, Estonia
Dubuis, Eric Bern University of Applied Science, Switzerland
Gibson, Paul Telecom SudParis, France
Gjosteen, Kristian NTNU Trondheim, Norway
Grechenig, Thomas INSO, Technical University Vienna, Austria
Grimm, Ruediger University of Koblenz, Germany
Gronke, Paul Reed College, USA
Haenni, Rolf Bern University of Applied Science, Switzerland
Hall, Joe Lorenzo CDT, USA
Hall, Thad University of Utah, USA
Imamura, Catsumi Centro Técnico Aeroespacial, Brazil
Kalvet, Tarmo Tallinn University of Technology, RNS, Estonia
Kersting, Norbert University of Muenster, Germany
Kim, Shin D. Hallym University, S.Korea
Kuesters, Ralf University Trier, Germany
Koenig, Reto Bern University of Applied Science, Switzerland
Nurmi, Hannu University Turku, Finland
Prandini, Marco DISI, University of Bologna, Italy
Pereira, Oliver Université catholique de Louvain, Belgium
Pomares, Julia CIPPEC, Argentina
Reniu, Josep Maria University of Barcelona, Spain
Rios, David Academy of Sciences, Spain
Ruggeri, Fabrizio CNR IMATI, Italy
Ryan, Mark University of Birmingham, United Kingdom
Ryan, Peter Y A University of Luxembourg, Luxembourg
Schneider, Steve University of Surrey, United Kingdom
Schuermann, Carsten ITU, Denmark
Schoenmakers, Berry TU Eindhoven, Netherlands
Serduelt, Uwe ZDA, Switzerland
Stein, Robert Federal MoI, Austria
Teague, Vanessa University of Melbourne, Australia
Tokaji, Dan Ohio State, USA
Trechsel, Alexander EUI, Florence, Italy
Wenda, Gregor Federal MoI, Austria
Wikström, Douglas KTH Royal Institute of Technology, Sweden
Zagorski, Filip University of Wroclaw, Poland
Zissis, Dimitris Aegean University, Greece

Conference Chairpersons

Krimmer, Robert Tallinn University of Technology, RNS, Estonia
Volkamer, Melanie Technische Universität Darmstadt, CASED, Germany

PhD Colloquium Chairpersons

Koenig, Reto Bern University of Applied Science, Switzerland
Barrat, Jordi EVOL2 - -eVoting Legal Lab / University of Catalonia, Spain

Organizational Committee

Traxler, Gisela E-Voting.CC, Austria (Main Contact)
Budurushi, Jurlind TUD, Germany
Meyerhoff Nielsen, Morten TUT, Estonia
Rincon Mendez, Angelica TUT, Estonia

Content

Experiences with Internet Voting

The Patchwork of Internet Voting in Canada

Nicole J. Goodman
Munk School of Global Affairs, University of Toronto
Toronto, Canada
nicole.goodman@utoronto.ca

Jon H. Pammett
Department of Political Science, Carleton University
Ottawa, Canada
jon.pammett@carleton.ca

***Abstract*— Internet voting developments in Canada are growing quickly, with activity focused in local elections, political party leadership votes and unions. In some instances, the federal structure of the Canadian state facilitates Internet voting use, while in others it inhibits it. The result of this system of divided jurisdiction is that Internet voting use in Canada resembles a patchwork, showing strong concentration in some areas and no penetration in other places. In addition to scattered geographic use, a variety of approaches to implementation are employed. In some cases online ballots are complementary to paper, while in others elections are now fully electronic. I-voting can be a two-step process requiring registration or a more direct one-step voting procedure. Likewise, Internet voting is offered in the advance portion of certain elections, whereas in others it is available for the full voting period. Finally, given that private companies administer the Internet voting portion of elections there is also a mixture of technology.**

Keywords—Internet voting; Canada; federalism; elections

I. INTRODUCTION

Canada possesses a multi-level governance structure[1], one where the various units often have effective control over their own electoral methods. This has resulted in a patchwork of Internet voting implementations within the country. Electoral Management Bodies (EMBs) with effective implementation power include Elections Canada (federal elections), provincial bodies like Elections Ontario, and offices of municipal government in hundreds of local areas. These agencies are subject to relevant legislation or regulations issued by federal and provincial parliaments, and by municipal councils. At times, this has resulted in instructions to implement trials of electronic voting methods, and in other instances specific prohibitions have been issued to prevent the use of such alternative voting methods. At other times, election agencies are left to make their own decisions, though they have usually sought approval from legislatures or councils before undertaking actual electoral trials.

This system of divided jurisdiction has resulted in the development of a substantial amount of Internet voting over the last decade. At the local level, nearly 2 million people have had opportunities to vote by Internet. These Internet elections have been concentrated in two provinces, Ontario and Nova Scotia. In Nova Scotia about one-third of communities have used Internet ballots, while in Ontario about one-quarter of the municipalities will do so in October 2014, comprising one-fifth of the provincial electorate. Supportively worded legislation in these provinces has enabled municipalities there to decide which voting methods to use. The Canadian constitution provides for overall provincial supervision (and ultimate control) of municipal governments. Municipalities are bound to carry out elections based on the framework established in *Municipal Elections Acts* written by the provinces. Providing a supportive legislative framework is in place, municipal governments have relative autonomy to implement experimental voting methods, and there is a substantial amount of local experimentation occurring.

This pattern is mirrored in another layer of Canadian governance, that of First Nations communities – bands of Aboriginal groups settled across the country. The overall system for governing First Nations elections is complex, but in many cases they are able to determine their own voting method. First Nations communities are now beginning to adopt Internet ballots in band elections and other types of votes such as referendums; to date they have been used in the provinces of Ontario and British Columbia.

Two further sets of Canadian institutions have made extensive use of Internet voting in their own internal operations. Many political parties at both the federal and provincial levels use the Internet to conduct leadership votes (local elections are nonpartisan), in keeping with the trend to choose their leaders by one person-one vote procedures involving the membership of the party [6]. Use of Internet voting for leadership votes is becoming so popular it is now the norm rather than the exception. Secondly, Canadian unions and professional/business associations have been steadily adopting Internet voting for their elections, with hundreds of these organizations making the switch to online ballots. Some Internet voting service providers report that these defined-group elections provide the bulk of their business [22].

II. INTERNET VOTING IN CANADIAN GOVERNMENTS

A. Federal Government

Federal elections in Canada are the responsibility of Elections Canada (EC). At present, EC is responsible for the administration of elections, regulating donations and campaign finances, and a variety of outreach and education initiatives. The bulk of its responsibilities surrounding the management of elections are laid out in the *Canada Elections Act* [4]. A bill recently passed in the House of Commons and now pending approval in the Senate, called the *Fair Elections Act*, made a number of changes to the role of the agency. Though Internet voting has not been trialed federally, current legislation requires that EC obtain approval from a parliamentary committee prior to moving forward. The *Fair Elections Act*, however, now requires that a provision for online ballot use be

[1] Federalism in Canada divides powers of government between national, sub-national and local levels, each which manage their own elections.

approved in both houses of the federal Parliament (including the unelected Senate), severely reducing the likelihood of Internet voting trials in federal elections.

EC has been researching Internet voting for some time and previously committed to carrying out a trial as part of its 2008-2013 Strategic Plan. Various operational considerations delayed this experiment, pushing the prospective trial back to 2015, and then again to 2019. Difficulties in relations between EC and the current Conservative government have made the agency more hesitant to undertake a trial, and it is now unclear when or if it will take place.

B. Provinces

Elections in Canada's ten provinces are administered by EMBs in each province. These are modelled on EC, led by a Chief Electoral Officer (CEO) accountable to the provincial legislature, and report to the legislative assembly either directly, through a committee, or in some cases via the Speaker of the House [15, 16, 18, 21, 23]. Various protocols surrounding the operation and management of provincial elections are outlined in pieces of legislation which typically include a primary *Elections Act*, an act pertaining to election finances, and various other regulations. In many cases EMBs have the authority to make recommendations to the provincial parliament.

No province currently has a legislative provision that would specifically permit the use of Internet voting in a general election; however, some have sections in their *Elections Act* that permit the CEO to test equipment in a by-election, which could allow an Internet voting trial. Elections Ontario, Elections Alberta, and Elections New Brunswick, for example, have such clauses in their *Elections Acts*. It is on this basis that Ontario plans to carry out an Internet voting trial in a future by-election. The introduction of these clauses has been part of a trend to support the modernization of electoral processes, perhaps triggered by declining voter turnout figures and needs to improve accessibility. Elections Alberta, for example, introduced new wording in 2008 to provide the opportunity for the CEO to test technology in hopes of modernizing the electoral process there [23]. Provinces without this section in their electoral legislation would need to have a provision added before proceeding with such a trial.

Most provincial EMBs have been researching the possibilities of Internet voting for about a decade, but trials have not occurred as early as originally expected. Elections Ontario, for example, was given a legislative mandate in 2010 to research 'network voting' and report back to the legislature, but this was pushed back due to financial considerations. Twelve interest groups were consulted in this process as well as the public through an online questionnaire. A report was issued in 2013, which suggested a test would not be as soon as expected [10]. Elections British Columbia recently issued a report that was the result of consultation with experts and some public input, whose findings recommend not proceeding with Internet voting at this time [9]. Elections Saskatchewan has taken a similar stance, issuing a public statement stating that online voting will not be implemented in the next general election (2015/2016). Smaller eastern provinces such as Prince Edward Island and New Brunswick have felt reluctant to be first to trial the technology and await the lead from a larger province. It seems Ontario has the greatest likelihood of proceeding with Internet voting in the near future. Because of online voting activity at the municipal level in Ontario, many of the province's electors have become familiar with this voting method.

Finally, we should note the lack of information and resource sharing among governments and between levels of government. There is some coordination at the top of EMB organizations, as the CEOs meet annually. Several provincial EMBs have come together in a national Electoral Voting Working Group facilitating some horizontal cooperation and information sharing regarding Internet voting, albeit the last meeting was held in 2012 [15]. At lower layers of the provincial bureaucracies, however, there is not the same institutionalized collaboration. Vertically, between national, sub-national, and local levels of government, there is not much dialogue either.[2] This lack of discourse has resulted in federal and provincial EMBs and local governments carrying out research and preparing reports in their respective silos. Even once a report is prepared, a series of internal approvals must often be sought before the document can be shared with other EMBs and governments, let alone the public. In the case of Ontario, for example, a Business Case for Internet voting was prepared, but the document was not available for sharing within the EMB community for six months, while approvals to circulate were obtained [21]. It is likely this lack of dialogue contributes to the patchwork of use and also implementation, explored below.

C. Municipalities

Municipal clerks have the responsibility to administer elections at the local level in Canada, and these local election officials have considerable independent authority to implement elections as they see fit.[3] This responsibility comes from the *Municipal Elections Act*. Clerks have the independent authority to determine how the election is administered, providing it complies with the requirements in the *Act*. However, some election aspects such as the voting method, the length of the advance voting period, and voting hours, must be approved by city councils before the administration can move forward [3]. In this sense local officials are bound not only by legislation written by the provinces, but also by the decisions of local councils when it comes to being able to implement Internet voting programmes.[4]

In their *Municipal Elections Acts,* at present, only the provinces of Ontario and Nova Scotia have clauses supporting the use of and/or experimentation with alternative voting

The authors would like to thank SSHRC for financially supporting the research.

[2] Saskatchewan started a program this year where the CEO of Elections Saskatchewan meets with six city clerks (five from larger municipalities and one from a more rural community) to discuss elections in the province. There is no standard format for how this will proceed, but it has provided a starting point for dialogue between the province and some municipalities [16].

[3] The one exception is the province of New Brunswick, which runs both provincial and municipal elections [15]. In some other areas (e.g. Prince Edward Island) the provincial EMB assists municipalities with the administration of elections [18].

[4] Municipalities are groups of communities that comprise a province. They range in population, population density, and land area and are responsible for the administration and delivery of local services.

methods. In British Columbia, municipalities including Vancouver and Nanaimo passed resolutions to enable the use of Internet voting, but were halted from moving forward when the province refused to support use of the voting method in local elections. The provincial election agency, Elections BC, assembled an independent electoral panel in September 2012 to advise on the possibility of using Internet voting for provincial and municipal elections. The panel eventually recommended to the provincial parliament that Internet voting not be implemented for local or provincial elections at this time [9]. In this way, the current structure of provinces controlling the legislation governing local Canadian elections has inhibited Internet voting as much as it has enabled it.

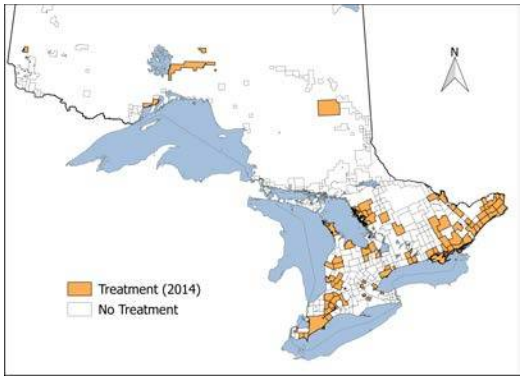
Municipalities in Alberta have been eager to pursue the use of Internet ballots in local elections. In 2012 the City of Edmonton, Alberta, conducted a mock online election (where voters cast a ballot for their favourite colour jellybean), and also conducted a public consultation through a public opinion survey and Citizens' Jury. These avenues of consultation indicated strong support for the use of Internet ballots in Edmonton's local elections, yet city council voted against the proposal. Seeing this, the provincial Ministry of Municipal Affairs declared a moratorium on Internet voting, thwarting the ability of communities still interested in its adoption, such as Grand Prairie, Wood Buffalo, and Strathcona County, from proceeding [8, 14]. In this case elected officials at both levels of government blocked the introduction of Internet voting.

In Ontario the province has put in place a legislative framework that supports the use of alternative voting methods and leaves the determination regarding types of ballots offered to the discretion of local government. A key example of cities adopting Internet voting has been the City of Markham, the first major Canadian municipality (over 100,000 electors) to use the technology. Officials in Markham supported Internet voting based on its perceived ability to enhance accessibility and convenience of the election process, improve voter turnout, focus on citizen-centered service, and to be recognized as a leader in e-government [19]. Another widely cited case involves the city of Peterborough, which has used Internet voting since 2006 [12]. Not all municipalities that consider the idea decide to implement it, however. Newmarket, Ontario is an example where the use of Internet voting was supported by city administration through research and planning and by the public through data collected from a household survey, but council voted not to allow its use in the 2014 elections. Part of this decision was due to concerns regarding security and privacy, but a lot of resistance developed from elected representatives who believed the option of Internet voting might encourage participation from electors who are not part of their voter base and typically abstain from elections (e.g. young people) [3].

In Ontario use of Internet voting in municipal elections has mushroomed. In 2003 twelve Ontario communities were the first to trial the technology. This number has increased with each round of elections growing to a potential of 98 communities out of 414 elections forthcoming in October 2014 representing about one fifth of the provincial electorate (see Fig. 1). In some cases, such as Markham, this has involved making online voting available in the advance voting period only, and included a two-step security procedure whereby electors were required to register to vote online to be able to access an Internet ballot [12]. In other situations, particularly elections in smaller municipalities (under 25,000 electors), Internet voting is offered during the entire election and does not require registration.[5] In these latter cases Internet voting is typically used in conjunction with telephone voting, making the entire election electronic. Larger municipalities (over 25,000 electors) have tended to stick with paper ballots and often only add Internet, excluding telephone. The result is a patchwork not only of adoption, but also Internet voting models.

In Nova Scotia, Internet voting use began in 2008 with four communities adopting the method, growing to fourteen in 2012. [6] Local officials have projected the number of communities offering online ballots will double in 2016, rising to 32 communities out of a potential 54 [24]. Much like Markham and other Ontario municipalities, motivations to introduce Internet voting have included becoming a leader in e-government, and improving access, convenience and electoral turnout [19]. In most Nova Scotia communities, with the exception of the provincial capital, Halifax, the Internet voting option has been kept open beyond the advance voting period to include election day. In a few cases, such as Digby Town, Truro, and Yarmouth, paper balloting on election day was done away with, and the entire election was carried out by Internet and telephone ballots

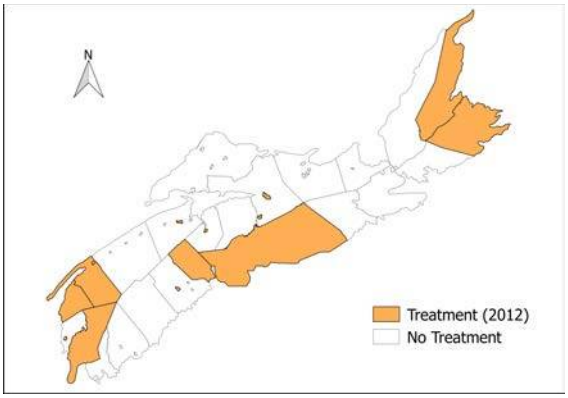
Though Internet voting has been adopted by some larger municipalities (Halifax, Markham) it is more likely to be used in smaller communities. It is especially favoured by communities that have large seasonal populations or have relied on voting by mail in the past. A majority of smaller communities use Internet voting for the full election, including election day. Fig. 1 and Fig. 2 depict Ontario and Nova Scotia municipalities that will have used Internet voting in binding local elections by October 2014, visually demonstrating the patchwork of adoption.



a. Sample Government of Ontario. Municipal Boundary - Lower and Single Tier. Ontario
b. Geospatial Data Exchange, Ministry of Natural Resources (OMNR), Peterborough, Ontario, Canada.

[5] It is important to note that 70 percent of Ontario municipalities have an electorate of 10,000 or less.

[6] Internet voting use was legally approved in sixteen Nova Scotia communities, however, only fourteen officially proceeded given that all seats in one area were acclaimed, and another determined they were unable to afford the cost at the last minute [11].



a. Sample of a Tab Government of Nova Scotia. Municipal Boundary File. GEONova, 2014.

D. First Nations

In the 617 First Nations communities in Canada, elections for Chief and band council can be governed in one of four ways (see Table 1). In 238 communities, the *Indian Act* (a federal piece of legislation) governs elections, with each participating First Nation community being responsible for carrying out their elections in accordance with the act. In April 2014, the *First Nations Elections Act* became law, providing another mechanism to govern elections in First Nations communities. This intent of this law was to create more modern electoral provisions than found in the *Indian Act:* some changes include longer terms in office, penalties for misconduct, and a common election day [13]. Communities can choose to opt-in to this legislation by passing a band council resolution, but it is presently unclear how many will do so.

A third approach to governing elections is the passage of Community or Custom Election Codes. These are election codes determined by the individual community with no interference from the federal government. Many of these codes are in fact derived from the *Indian Act*, but have been amended by communities [2]. An example of an amended provision includes the ability for off-reserve members to vote in band elections. The original wording of the *Indian Act* only allowed for First Nations members living on-reserve to cast a ballot and many communities wanted all members to be able to participate. This provision was challenged legally and the Supreme Court of Canada ruled that it violated the *Canadian Charter of Rights and Freedoms* and was unconstitutional [5]. As a consequence both on and off-reserve community members have been able to participate in Chief and council elections ever since. This change in the number, and nature of, eligible voters prompted the use of mail-in ballots in many communities. Internet voting is now appealing to many bands with large off-reserve populations that presently rely on vote by mail [2]. 2014 saw large increases in Canadian postal rates, and the beginning of a phase-out of home mail delivery, developments which will likely accelerate interest in Internet response alternatives.

Finally, 36 First Nations are considered self-governing. These communities develop their own laws to govern elections independent of any outside government and these codes are usually unique to each community based on their needs [13]. Typically, self-governing communities are distinguished by the fact that they have expanded law making authority [2].

The Indian Act and First Nations Elections Act are written to provide for paper ballots and vote by mail as methods. The ability to introduce online ballots would require a provision be added to these pieces of legislation. Communities with custom codes and those that are self-governing, however, may choose to introduce Internet voting by passing their own resolutions.

TABLE I. FRAMEWORKS FOR FIRST NATIONS ELECTIONS IN CANADA

Legislation	***# of Bands***
Indian Act and *Indian Band Election Regulations*	238
Custom and community election codes	343
Self-government agreements	36
First Nation Elections Act	*To be adopted, passed April 2014*

As the above table indicates, 379 bands could now use Internet voting methods. Overall tabulations of how many now do so, or are intending to do so, are not yet available. Some examples do exist, however. Several bands in the provinces of Ontario and British Columbia have used i-voting for various referendums and votes, although online ballots have yet to be used in a binding contest to elect band government. Nipissing First Nation, in Ontario, used Internet voting to complement paper and mail-in ballots to ratify their own constitution between November 2013 and January 2014 [7]. In British Columbia, a number of votes have taken place by Internet. Squamish First Nation used online ballots in March 2013 for a membership amendment referendum. One self-governing community in British Columbia, the Huu-ay-aht First Nation, has explicitly included a provision in their *Election Act* (Section 49(1)) to permit the use of electronic types of voting [17]. In September and April 2011 Talhtan First Nation used Internet ballots for votes regarding band member status and the introduction of power transmission lines. Talhtan will become the initial First Nation community in Canada to elect its band representatives by Internet in July 2014 [22].

Associations of First Nations are also beginning to make use of Internet ballots. The Union of Ontario Indians, an organization representing 39 First Nations communities, conducted a public consultation of all its members in early 2014 concerning a controversial piece of education legislation crafted by the federal government. Much like at the municipal level, the varied pieces of legislation governing elections provide the foundation for a relative patchwork of adoption. Providing communities have their own codes to govern elections, they are free to move forward with the implementation of digital technology with support from band council. Internet voting appeals to First Nations communities given the presence of sizable off-reserve populations (in many cases two thirds of band members live off-reserve). Even if Internet access and connectivity is an issue, online ballots may still be adopted to facilitate accessibility for those who live off the reserve lands [2].

III. INTERNET VOTING AND OTHER ACTORS

A. Political Parties & Unions

Federal and provincial political parties have been gravitating toward the method to facilitate their leadership votes. These organizations are free to use election methods as they see fit and have the power to introduce Internet voting providing it is permitted by their constitution. Internet voting is particularly attractive to parties to combine with, or replace,

TABLE II. POLITICAL PARTY LEADERSHIP VOTES USING I-VOTING

National (Canada)	Date	Overall Turnout	Methods	Use of Method
New Democratic Party	January 2003	54%	P, T, I	N/A
	March 2012	71%	P, I	
Liberal Party of Canada	April 2013	82.2%	I	82.2% I
Sub-national (province)				
Alberta Party	May 2011	58.7%	I, T	49.9% I 11.8% T
	September 2013	58.1%	I, T	50.7% I 7.4% T
Liberal Party of Alberta	September 2011	29.8%	I, T	21.2% I 8.6% T
Liberal Party of British Columbia	February 2011	62.4%	I, T	51.4% 11% T
British Columbia NDP	April 2011	71.3%	I, T	48% I 23.3% T
	September 2014	ACC	I, T	ACC
New Brunswick Liberal Party	October 2012	78.5%	I, T, M	38.8% I 15.1% T 24.5%M
Newfoundland & Labrador Liberal Party	November 2013	62.8%	I, T	30.5% I 32.3% T
Ontario NDP	March 2009	55%	I, T, M	25.4% I 4.6% T 25% M
Saskatchewan NDP	June 2009	72.4%	I, T, M	20.2% I 6.1% 46.1%M
	March 2013	77.9%	I, T, M	44.1% 7.6% T 48.3%M
TOTAL		**Avg**		**Avg i-vote**
12 parties, 8 provinces, 3 national votes	13 leadership votes	64%		41.8%

[a.] Please note "I" represents Internet voting, "T" represents telephone voting, "M" denotes vote by mail, "P" recognizes the use of paper ballots, "ACC" stands for acclaimed, and "N/A" not available.

voting by mail. To date a combination of vote by mail, Internet, and telephone ballots have been used to facilitate thirteen national and provincial leadership votes (see Table 2), with two additional e-vote elections expected in the coming months. Although first trialed in 2003, it has only been used regularly since 2009. Mostly center and left of center parties have been attracted to online voting, while comments from conservative organizations often focus on how the introduction of Internet voting may encourage participation from those who are not typically part of their membership base (e.g. young people). Two provincial conservative parties are considering Internet voting, however. The Progressive Conservatives in Prince Edward Island will likely use online ballots in their fall leadership election, and the Alberta Conservative Party is contemplating use for their upcoming leadership vote [1]. Overall, Internet voting appears to have helped improve turnout for these types of votes and seems to be the preferred method of participating for party members.

Unions representing blue and white collar workers have also embraced i-voting as a means of engaging members in elections and other votes. There are four levels of unions in Canada: international unions, national unions, regional unions, and local unions. I-voting is being explored by unions at all levels, but there is greatest interest at the local and regional levels. Online ballots have been used to date for union strike votes, ratification votes, collective bargaining, and union elections. In some cases local levels of unions are free to implement i-voting in elections, while in others they require approval from the national body [20].

B. Internet Voting Vendors

All the Canadian Internet elections held so far have been contracted to private companies, hired to carry out the electronic portion of the election. Six companies currently provide service in Canada: CanVote, Dominion Voting, Everyone Counts, Intelivote, Scytl, and Simply Voting. CanVote, Intelivote, and Simply Voting originated in Canada, while Dominion Voting and Everyone Counts are American, and Scytl is headquartered in Spain. In 2003 CanVote and an American company, Election Systems & Software, provided e-ballot service in Canada. Since then there has been an influx of companies providing a wide range of election services, including online poll training for workers, modules for candidates to track whether electors have voted (but not who they voted for) and target their get out the vote efforts. It is worrying to some that there are currently no minimum security standards in Canada for these elections, although some larger companies have been pushing for these regulations. In terms of Canadian market share Intelivote seems to lead the pack having hosted ten party leadership votes and securing 50 percent of municipal business for 2014. Scytl has carried out two leadership votes, Dominion Voting one, and each have about a quarter of the municipalities offering Internet voting subscribing to their services. The remaining companies hold less than five percent of municipal business.

IV. CONCLUSION

Canada's Internet voting deployment resembles a patchwork in a number of respects. First, most activity takes place at the local community level in two of the ten provinces, with a considerable amount in some other political organizations. The nature of divided jurisdiction and division of electoral powers has in some cases prevented the use of Internet voting, but in others the presence of supportive legislation and local autonomy has allowed its implementation. Second, the relative sovereignty of local councils to implement election changes, providing these adhere to the legislative framework written by the provinces, means that councils which have adopted Internet voting have taken a variety of approaches to implementation. This includes differences regarding the portion of the election in which i-voting is offered (e.g. advance poll or full election), and in the steps that

must be taken for an elector to cast an online ballot (e.g. whether online registration is required or not). In some cases paper ballots continue to be offered, while in others local elections have converted to being completely electronic. Limits in horizontal communication (within levels of government) and vertically (between them) has handicapped information sharing and hindered consistency in adoption and the type of model deployed.

In addition, there is a relative patchwork of technology employed given the different companies in the market and their e-voting solutions. While levels of government in other federal states considering or actively using Internet voting (such as the US and parts of Europe) have come together and implemented certification standards related to security, there is currently no such model in Canada. A lack of standards has caused concern regarding the level of security surrounding municipal elections, especially since governments with smaller budgets may be inclined to award contracts to vendors on the criterion of price. The result is a mixture of security standards regarding the Internet portion of the election.

In sum, there is a considerable amount of Internet voting in Canada. Various elements of the federal structure of authority and the decisions of local authorities have enabled Internet voting use to prosper in some areas, while in others development has been suspended. In one sense, a variety of 'policy laboratories' has allowed considerable innovation, but in another, the lack of consistency and standards provides cause for concern.

ACKNOWLEDGMENT

The authors thank SSHRC for financially supporting the research.

REFERENCES

[1] B. Anderson, Councillor, City of Edmonton. Personal interview, May 16, 2014.

[2] F. Bellefeuille, Legal Council, Union of Ontario Indians. Personal interview, May 9, 2014.

[3] A. Brouwer, Clerk, Town of Newmarket. Personal interview, February 3, 2014.

[4] *Canadian Elections Act* (Government of Canada), Act S.C. 2000, c. 9.

[5] Corbiere v. Canada (Minister of Indian Affairs), [1999] 2 S.R.C. 203.

[6] W. P. Cross and A. Blais, Politics at the Centre: The Selection and Removal of Party Leaders in the Anglo Parliamentary Democracies. Oxford University Press, 2012.

[7] S. Crutchlow, General Manager, Scytl Canada Inc. Personal communication, December 6, 2013.

[8] City of Edmonton, Report to Council – 2013 Municipal Election, 2013.

[9] Elections BC, Independent Panel on Internet Voting: Recommendations Report to the Legislative Assembly of British Columbia. British Columbia, February 2014.

[10] Elections Ontario. Alternative Voting Technologies Report: Chief Electoral Officer's Submission to the Legislative Assembly. Ontario, June 2013.

[11] N. Goodman, "Internet voting in a local election in Canada", in *Internet and Democracy in Global Perspective*, Studies in Public Choice 31, Eds. Bernard Grofman, Alex Trechsel, and Mark Franklin, Springer Verlag, 2014.

[12] N.J. Goodman, J. H. Pammett, and J. DeBardeleben, A comparative assessment of electronic voting, Elections Canada, 2010.

[13] Government of Canada, "Fact sheet – understanding First Nation elections" Department of Aboriginal Affairs and Northern Development, 2014: https://www.aadnc-aandc.gc.ca/eng/1323193986817/1323194199466 Last accessed: May 27, 2014.

[14] D. Griffiths, Minister of Municipal Affairs, Province of Alberta. Personal communication, March 6, 2013.

[15] P. Harpelle, Director of Communications & Community Outreach, Elections New Brunswick, May 9, 2014.

[16] T. Kydd, Senior Director, Outreach & Policy, Elections Saskatchewan. Personal interview, May 9, 2014.

[17] P. MacWilliam, *Online Voting in Local Government Elections*. University of Victoria, 2014.

[18] G. McLeod, Chief Electoral Officer, Elections Prince Edward Island. Personal interview, May 9, 2014.

[19] J.H. Pammett, and N. Goodman. Consultation and Evaluation Practices in the Implementation of Internet Voting in Canada and Europe. Ottawa: Elections Canada, 2013.

[20] M. Pivon, Sales Director, Western Region, Scytl Canada Inc. Personal interview, May 27, 2014.

[21] S. Pollock, Director, Technology Services, Elections Ontario. Personal interview, March 29, 2014.

[22] D. Smith, President, Intelivote Systems. Personal interview, May 13, 2014.

[23] D. Westwater, Director of Election Operations and Communications, Elections Alberta. Personal interview, May 9, 2014.

[24] B. White, Municipal Clerk and Returning Officer, Cape Breton Regional Municipality. Personal communication, December 17, 2012.

iVote.lt - a practical attempt to overcome online voting - related fears

Jonas Udris
Election Law Expert
Vilnius, Lithuania
jonas@sutartys.lt

Abstract - The paper presents the first practical attempt to introduce the advantages of online voting to the general public, offering a fully functional prototype that covers every major aspect of the online voting procedure. The authors believe that the success of this project will ease the fears and remove the doubts related to the introduction of online voting in binding elections.

Keywords—online voting, Lithuania, ivote.lt, simulator

I. THE SHORT OVERVIEW

iVote.lt is the first Lithuanian online voting simulator, which was aimed to promote and popularize online voting. The project took place prior to the official Parliamentary elections of 2012 and was hosted by www.delfi.lt, the largest Lithuanian online news portal. A total of 3566 people tested iVote.lt, which is three times as many needed for a sociological survey. More than 30 000 people at least tried the simulator; i.e., they have read the description, viewed the presentation, and downloaded the simulator software. This is more than number of voters required for one constituency. Ninety-eight percent of participants of the project voted "Yes" for introducing online voting in Lithuania.

II. INTRODUCTION

First attempts to introduce online voting in Lithuania took place in 2005, when the Concept (Draft Law) on Internet Voting was prepared by the Central Electoral Commission (CEC) and presented to Parliament [1]. Since then, multiple initiatives aimed to introduce online voting did not pass the submission stage in Parliament. Those initiatives were supported in many public, academic, and political discussions, but none led to any tangible results.

Despite the technological progress of Lithuania - where Internet speeds are among the fastest in the world, Wi-Fi hotspots grow like mushrooms in the forest after the rain, people no longer go the Tax Inspectorate in person, and banks close their offices due to the lack of visitors - online voting is still far beyond the horizon. Politicians and some part of the public believe in urban myths like "every computer system is hackable", and that online voting would lead straight to widespread electoral fraud.

To scatter these myths and increase public confidence in the idea of voting online, encourage politicians to overcome their fears, and introduce this modern way of voting, this fully-functional online voting simulator was created and introduced to the Lithuanian public in September 2012, four weeks before actual parliamentary elections. It was called the "iVote.lt project".

The goal of this paper is to present the iVote.lt project and explain how it helped increase public confidence in online voting.

III. THE IDEA

The idea was to put together the knowledge of CEC officials, the power of popular online media, and the capability of a team of programmers in order to present a working simulator that demonstrated and allowed people to try this new way of casting their vote. The simulation game invited people to try the online voting and help resolve all the myths and doubts that surrounded this way of casting a vote in real elections and referendums of the future.

The simulator had to demonstrate that online voting could be a secure and reliable voting method that fully complies with the democratic election principles set in the Constitution, the election laws, and international standards of free and democratic elections. Among those principles are the following: Free elections, Secret voting, Equal voting rights, Audibility, Reliability, Flexibility, Uniqueness, Integrity, and Convenience [2].

The project was started in January of 2012 by online voting enthusiast CEC member Jonas Udris and online media producer Justinas Vanagas. They defined the scope and aim of the project. A private IT company, UAB "EVP International", which specializes in creating online payment systems, was invited to join the project. The owner, Mr. Kostas Noreika, kindly agreed to help and appointed a team of programmers to code the software of the simulator.

The Central Electoral Commission, the Minister of Transport and Communications, and the Minister of Justice expressed their moral support for the project, and the State Enterprise Center of Registers kindly allowed the project to use their online identification system, www.ipasas.lt.

Technically, ivote.lt was based on early versions of the Estonian online voting model [3]. During the design phase many legal, information technology and election specialists contributed their knowledge and expertise to the project. The authors also tried to follow to the Recommendation Rec(2004)11 of the Committee of Ministers to member states

on legal, operational, and technical standards for e-voting [4].

The project followed exclusively informational and educational objectives. It was not part of any election campaign and did not mean to promote any political party or power. The people behind the project were not politically biased and did not belong to any political power. The project had no aim to influence election results in any way.

The simulator was not designed to imitate the real upcoming elections of 2012 or to predict their outcome. It was designed to motivate the society to show their interest in online voting as an alternative way of casting a vote.

The results of the game were completely anonymous; therefore, personal political preferences of the participants were not made public. Some statistical information was presented as additional information, such as the distribution of the voters by age, gender, and geography.

IV. The Design

The main idea behind the iVote.lt project was the "double envelope" voting principle, which is basically a digital version of traditional advanced voting by post. The voting process consisted of five major steps: 1) Generating a pair of keys; 2) Filling the ballot and encryption; 3) Casting the ballot; 4) Anonymisation; 5) Decryption and tabulation of the results.

The simulation game was designed following the principles of transparency and auditability. Therefore, only well-known and open-source libraries were used:

- The www.ivote.lt website was created using open source Symfony2 carcasus; HTTPS protocol was used.
- www.ipasas.lt of State Enterprise Center of Registers was used for user authentication.
- Java Web Start application (JRE 1.5 version and up). The source code signed by Code Signing certificate.
- Bouncy Castle Crypto (http://www.bouncycastle.org/java.html) API was used to encrypt the ballot. Data was then put to a CMS Enveloped Data package and encrypted with a 128 bit key.

The source code of the project was open for public download.

A. Generating the pair of keys

First, the pair of digital keys was generated. The Public Key was uploaded into the system and the Private Key was deconstructed and put away for safekeeping until the end of the voting. Parts of the Private Key were burned onto blank CD's and distributed among organizers of the simulator.

B. Filling in the ballot

The voting simulator was accessible either directly at www.ivote.lt or via the news portal www.delfi.lt, where it was widely advertised. The user was offered the download of a small JAVA applet, which contained an electronic "ballot" and a questionnaire, together with an encrypting algorithm and a Public Key. There was no need for any specific IT knowledge or software installation to use the simulator. The simulator worked on all JAVA-supporting operating systems, including Windows XP and higher and Mac OS X version 10.6 and higher.

Once the user finished "filling in the ballot" and the questionnaire, he or she was then asked to click a button that read "Encrypt the ballot". After the encryption was complete, the binary file containing encrypted information was generated and saved onto the user's desktop. This binary file did not contain any personal data or any other data that, when decrypted, could link the "ballot" to the voter's identity. The file name contained only the date and time of the file. The "ballot" could be opened in any text editor, but it looked like lines of random characters.

Thus, the filled out ballot and data encryption were completely anonymous; no personal or other identifying information was stored in the encrypted file. If one wanted to be sure of anonymity, he or she could transfer the encrypted file to another computer and submit it from there.

C. Casting the ballot

Once the encrypted file was generated, the user was asked to choose the "Cast the ballot" function and then they were forwarded to the www.ipasas.lt website for authentication. Here his or her identity was determined using an online banking system or a digital signature. After the authentication was complete, the user was asked to upload his or her encrypted vote. As the "ballot" file was encrypted and the private key was not accessible, no one, even the administrators, were able to disclose the persons' "vote". The user could upload as many ballots as he or she wanted, but only the last vote counted. The previous votes were destroyed (overwritten).

Some of the data, such as the voter's age, gender, and IP-based location, was collected separately for statistic purposes.

The "last vote counts" principle was achieved in a very simple way using some basic principles of computer operating systems: two files with the same name cannot exist in the same folder. When the person identified himself or herself to the system, a unique number (a long integer) was generated based on the voter's personal code using a Hash function; thus, a unique number was created for each voter but the voter could not be identified backwards. This unique number was used as a file name to the encrypted ballot. So, after the voter authenticated himself or herself and uploaded the encrypted ballot file, the ballot file got a unique name generated by "hashing" the voter's personal code. Every other vote cast by the same voter got the same file name;

thus, it automatically overwrote the previous vote. This means that only the last vote is stored in the database, with no history (unless the database is somehow duplicated or backed up before the vote update). This allowed the existence of the "cancellation vote", a special instruction that could be sent to the server to delete the vote that was previously cast.

This explanation of the "last vote counts" principle was the easiest way to convince people that the ballots were actually not linked to the voter's identity, and there really was no way to disclose the secrecy of the vote in this phase.

A Youtube video [5] was made to demonstrate how the simulator worked.

V. The process

The simulation voting was launched on the 18th of September, 2012 at 12:00 after an announcement on www.delfi.lt, the largest Lithuanian news portal. An immediate reaction followed the launch. The promotional article was read more than 40 000 times, and readers left more than 1000 comments in just the first few hours.

More than 600 people tried the simulator on the first day.

The voting lasted for 17 days – until the 5th of October, 2012. A total of 3788 electronic "ballots" were uploaded (including "re-votes"). More than 30 000 users downloaded the voting application but never uploaded the ballot.

One hundred and two participants "re-voted" at least once. A total of 3566 valid ballots were counted.

One hundred and fifty-eight users downloaded the source code.

Every voter was offered a Certificate of Participation. (This was a generated PDF file with the user's name and surname, saying that he or she had participated in the first educational online voting simulation game.) The mayor of Vilnius and several ministers and members of Parliament were among those who proudly published their certificates on their Facebook timelines.

VI. Anonymisation, decryption, and tabulation of the results

After the "voting" period was over, the collection of votes was stopped and the anonymisation process started. The server with all of the "votes" was disconnected from the Internet first.

The process worked by simply randomizing the filenames of the ballot files. As we did not store a history of the votes, we had only the last "valid" votes; thus, randomization of the filenames was sufficient to ensure voter anonymity and that only one vote per voter was counted.

The Private Key was put back together and the decryption algorithm was then launched. The votes were decrypted and the results were then tabulated. The Private Key was then destroyed so any previously made (or backed-up) copies of the votes could not be decrypted.

VII. The results overview

As this simulation was widely supported by liberal-wing politicians and youth organizations, liberal (28,86%) and conservative (26,00%) parties "won the online elections". Of course, this did not correspond to the results of the actual elections of the Parliament that took place the week after the simulator ended.

Voter distribution was as follows:

- 1130 females (30 percent) and 2638 males (70 percent),
- 679 voters ages 18-24,
- 1603 voters ages 25-34,
- 861 voters ages 35-44,
- 408 voters ages 45-54,
- and 215 voters ages 55 and above.

Although the simulator covered most aspects of online voting protocol, some important aspects were missing and should be resolved before introduction in binding elections.

Firstly, anyone with a Lithuanian electronic ID or means of internet banking authentication could participate in the ivote.lt project, regardless of their citizenship or age. Only the ones included in the electronic voters' list could vote in real online voting.

Secondly, the ballots of the iVote.lt were all the same, and the person that downloaded this was completely unknown to the system. In real voting the voter would first identify himself or herself electronically, so the ballot issuing server could determine if he or she were eligible to vote and voting constituency, and then give him or her the respective ballot.

Thirdly, it was possible to authenticate to iVote.lt not only by digital signature, but also by means of internet banking. In real online voting internet banking is not a valid method of authentication. The voter would sign in using a digital signature or other means of electronic ID, depending on the legal framework.

Fourthly, ivote.lt did not offer an option for the voter to check if his or her vote was counted, which is becoming a standard in actual working online voting systems.

All other technological and organizational methods, including "The last vote counts", "Vote cancellation", and user interface meets the requirements for online voting systems, so it is only a matter of time and political will when this voting method will be implemented in our country.

VIII. Publicity and media coverage

As noted before, the ivote.lt was not only a piece of software, but also a publicity project. More than 20 popular articles were published on the major Lithuanian news portal delfi.lt, where different people (politicians, bankers, artists, scientists, and others) expressed their support for the

introduction of online voting. There were also articles on cyber-security, digital signatures, and digital identity.

Three big rounds of discussions were held in the headquarters of the Central Electoral Commission. All three events were webcasted live on the Internet and video reviews were made after. The first round gathered representatives of the media, business, and politics. The second round brought together all the leaders of the main political parties, and the third round included IT experts, journalists, and representatives of the expatriates. These discussions revealed the growing demand of society to introduce online voting, especially among expatriates and young, active people living in Lithuania. The IT experts agreed that the current IT infrastructure is sufficient to ensure the required level of security, but some politicians still expressed a high level of mistrust and kept declaring that "our society is not ready yet".

IX. Conclusions

The project was created to promote the idea of online voting and to explain to the general public how online voting might work. The users were able to test the possibilities and advantages of online voting by themselves.

The following conclusions were made:

1. More than 3500 people participated. That was twice as many as the authors initially expected.
2. The main objective of the project was achieved completely; i.e., a fully operational online voting module was presented to the public. It scoped every aspect of online voting procedure – starting with user authentication and vote encryption, and ending with depersonalization and tabulation of the results.
3. The project proved that anonymity of the vote can be guaranteed during all stages of online voting. This was clearly explained to the public.
4. Despite the fact that results of ivote.lt do not correspond with the actual results of the Parliamentary elections of 2012, wide distribution of votes among parties show that online voting is supported by citizens of various political views.
5. The geographical distribution of ivote.lt participants showed there is a possible increase in turnout of voters living abroad.
6. The gender and age statistics showed that online voting is supported by various ages among both genders.
7. The project drew a lot of attention from various fields of society and government; politicians, businessmen, journalists, and other public figures joined the online voting–related discussions.
8. Despite a number of attempts, we do not have any information that the system was ever hacked or influenced from the outside in any way.

X. Further Steps

The online voting simulator drew enough public attention to the idea of online voting. Despite obvious Estonian success, the introduction of online voting in Norway, and online voting for expatriates in France, there is still a lot of resistance and doubt among politicians regarding the introduction of online voting in Lithuania.

However, there have been small steps made in the right direction. For the first time ever, during the presidential elections of 2014 the candidates were able to gather signatures of their supporters online. The winner - current President Dalia Grybauskaitė - collected the required minimum of 20 000 signatures just online. A total of more than 60 000 signatures were collected online. This shows growing public confidence in e-democracy.

The amendment to the Law on Municipal Governance was submitted to the Parliament, which will allow anonymous public surveys (i.e., local referendums) by means of electronic communication. This will allow the creation of a fully-functional online pilot system that technically will meet all the requirements for national elections, and could be tested and evaluated without putting national-level elections at risk.

In the spring of 2014 the Minister of Justice, together with the Minister of Transport and Communications, announced that online voting will be introduced in Lithuania some time soon.

References

[1] First Lithuanian concept for internet voting. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=287235&p_query=&p_tr2=

[2] Electronic Voting: Algorithmic and Implementation Issues, Robert Kofler, Robert Krimmer, Alexander Prosser, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).

[3] http://neu.e-voting.cc/wp-content/uploads/Proceedings%202006/1.1.madise_martens_e-voting_in_estonia.pdf

[4] Recommendation Rec(2004)11, adopted by the Committee of Ministers of the Council of Europe on 30 September 2004, was prepared by the Multidisciplinary Ad hoc Group of Specialists on legal, operational and technical standards for e-voting (IP1-S-EE).

[5] A link to a Youtube video, explaining how the simulator worked: https://www.youtube.com/watch?v=8akH1g0Iug4

[6] http://www.coe.int/t/dgap/democracy/Source/EVoting/EVotingReview06/JONAS%20UDRIS-Strasbourg2006.ppt

Verifiable Internet Voting in Estonia

Sven Heiberg*† and Jan Willemson*‡
*Cybernetica, Ülikooli 2, Tartu, Estonia
†Smartmatic-Cybernetica Centre of Excellence for Internet Voting, Ülikooli 2, Tartu, Estonia
‡Software Technology and Applications Competence Centre, Ülikooli 2, Tartu, Estonia
Email: {sven,janwil}@cyber.ee

***Abstract*—This paper introduces an extension to the Estonian Internet voting scheme allowing the voters to check the cast-as-intended and recorded-as-cast properties of their vote by using a mobile device. The scheme was used during the 2013 Estonian local municipal elections and the 2014 European Parliament elections. 3.43% and 4.04% of all Internet votes were verified, respectively. We will present the details of the protocol, discuss the security thereof and the results of implementation.**

Keywords*—*Verifiable electronic voting

I. Introduction

The first legally binding elections allowing votes to be cast over the Internet took place in 2000 at the University of Osnabrück, Germany [1], and in Arizona, USA [2]. Just five years later, Internet voting was used in the Estonian countrywide local municipal elections [20]. Since then, legally binding Internet voting has been applied by various other countries and organizations, e.g. the Austrian Federation of Students [18], Switzerland [4], Netherlands [15], Norway [27], etc.

Several of the abovementioned implementations have encountered some security issues. For example, as a response to Arizona pilot, it was recommended to delay Internet voting until suitable criteria for security are put in place [24]. The Austrian Student Federation election of 2009 was subject to a DDoS attack [10]. Both the 2011 and 2013 attempts to introduce e-voting in Norway suffered from software and physical implementation errors [27], [8]. The 2011 Estonian elections were subject to several attacks including a proof-of-concept vote manipulation malware and politically motivated attempts to revoke the results of the whole electronic vote [13].

Electronic voting can be considered inherently more dangerous compared to conventional paper-based voting, as the lack of physical evidence creates the need to trust the electronic voting device. A buggy or malicious voting device could tamper with the electronic ballot without anybody being able to detect the manipulation. If the voting device and the digital ballot box communicate over the Internet, they are exposed to geographically unbound, highly scalable attacks from the network. A security analysis for an Internet voting system provided by SERVE (Secure Electronic Registration and Voting Experiment) suggested that Internet voting should not be attempted, unless some unforeseen security breakthrough appears [16].

Verifiable voting protocols attempt to improve the situation by providing participants with the ability to check whether certain properties hold on, e.g. the electronic tally. If the protocol gives voters the means to check the properties of their individual ballots, we can refer to an *individually verifiable* voting protocol. For example, it might be possible for the voter to check whether the electronic ballot cast over the Internet was correctly accepted by the digital ballot box. There are several protocols that provide some kind of verifiability to Internet voting [26], [5], [17], [11].

In this paper, we present an individually verifiable protocol that was used in the 2013 Estonian local municipal elections and the 2014 European Parliament elections. The paper is organized as follows. Section II describes the basic Estonian Internet voting scheme and explains the need for verifiability, and Section III defines the exact objective for the verifiability extension proposed in Section IV. Section V discusses the provided security guarantees together with the residual risk vectors, and Section VI gives practical implementation results. Finally, Section VII draws some conclusions and sets out the direction of future work.

II. Estonian Internet voting in 2005–2014

The Estonian Internet voting scheme was developed in the early 2000s and is described in detail in [13]. It has been used at seven elections during 2005–2014 and the basic protocol has remained essentially unchanged.

On the conceptual level, the scheme is very simple and mimics double envelope postal voting. The central voting system generates an RSA key pair and publishes the public part s_{pub}. The voter v authenticates herself for the voting server using her ID card or mobile ID (standard identification mechanisms widely used in Estonia), and receives the candidate list. She then makes her choice c_v (which is just a candidate number in case of Estonian elections) and encrypts it with the server's public key. For encryption, RSA-OAEP is used and a random seed r is generated for the cryptosystem. Hence the anonymous ballot ("inner envelope") is computed as $b_{anon} = Enc_{s_{pub}}(c_v, r)$. The effect of the "outer envelope" is achieved by signing the ballot using the voter's ID card, and the resulting complete ballot $b = Sig_v(b_{anon})$ is sent to the voting server (see also Figure 1).

The scheme uses re-voting as an anti-coercion measure. The voter can cast a vote over Internet several times, but only the last vote will be included in the tally. This way, if a voter feels coerced, she can re-vote later. The voter can also vote on paper to cancel her electronic vote. It is assumed that uncertainty in

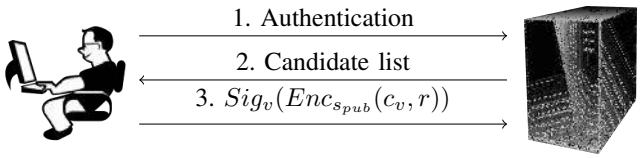


Fig. 1. The basic Estonian Internet voting protocol

the outcome of the coercion attempt makes such attempts an inefficient attack vector.

Electronic ballots are kept in the signed and encrypted form until the voting period is over. The signatures are then dropped and anonymous ballots are tallied; for that, they are decrypted with the server's private key stored in a hardware security module.

While it is rather straightforward, the system has several weaknesses, some of which were exploited during the 2011 parliamentary elections. The most severe and widely published attack was proposed by a student who made use of the fact that in its original form, the voting system gave no reliable feedback concerning whether or how the vote was actually received by the server. The student developed several versions of malware capable of blocking or even changing the vote. Due to the simple nature of the basic protocol, such manipulations would remain unnoticed by the voter [13].

After the 2011 elections, these issues were addressed in the OSCE/ODIHR report [22]. Among other suggestions, the report states:

> *The OSCE/ODIHR recommends that the NEC forms an inclusive working group to consider the use of a verifiable Internet voting scheme or an equally reliable mechanism for the voter to check whether or not his/her vote was changed by malicious software.*

The current paper can be seen as a direct consequence of this suggestion, presenting a scheme that allows the users to verify the correctness of their votes. The scheme was implemented and used as a pilot during the 2013 Estonian local municipal elections and the 2014 European Parliament elections.

However, adding vote verifiability to the system may have unexpected side effects which can violate other requirements of the election. For example, the Council of Europe has published its recommendations on legal, operational and technical standards for e-voting [3]. Recommendation number 51 reads:

> *A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.*

It can be argued that any sufficiently strong form of vote verification may be used as a proof of the content, and hence facilitate vote selling or coercion, for example [7]. In the current paper we assume the hypothesis that the truth lies somewhere in between and try to propose one possible trade-off between verifiability and coercion-resistance. See Sections V-B and V-C for a more detailed discussion.

III. Types of verifiability

There is no generally accepted definition of the verifiability of electronic voting. Various authors define it differently depending on the needs and capabilities of the community setting up the elections. We refer to [19] for a good overview and comparison of the proposed approaches. In this paper, we will rely on the definition given by Popoveniuc *et al.* [23]. They define end-to-end verifiability through the performance requirements set for the voting system. An end-to-end verifiable voting system will provide the following properties:

1) The voter is able to check that her ballot represents a vote for the candidate to whom she intended to give the vote.
2) Anyone is able to check that valid ballots do not contain over-votes or negative votes.
3) The voter can check that her ballot is recorded as she cast it.
4) Anyone is able to check that all the recorded ballots have been tallied correctly.
5) Anyone is able to check that the voters and the general public have the same view of the election records.
6) Anyone can check that any cast ballot has a corresponding voter who can perform check No. 3.

Popoveniuc *et al.* also analyze several proposed systems and conclude that some of them are fully end-to-end verifiable (e.g. Prêt à voter [25] or Scratch & vote [6]). Some other systems (e.g. Scantegrity II [9] or Helios [5]) need one of the requirements to be slightly relaxed.

We will not be requiring end-to-end verifiability in the full sense of Popoveniuc *et al.* for the Estonian voting system. We will only require the individually verifiable properties 1 (cast-as-intended) and 3 (recorded-as-cast) from the list above. There are several reasons for that. First, the 2011 parliamentary elections showed client-side weaknesses both in the preparation and transport of ballots. Cast-as-intended and recorded-as-cast properties address these weaknesses. This is similar to conventional paper-based elections that have these properties under certain assumptions, namely that:

1) The voter is capable of representing her choice correctly;
2) The ballot paper and the ballot marker pen are not tampered with and perform their function correctly;
3) The voter personally takes the ballot from the polling booth to the ballot box.

From this point on, the voter has to rely on the election officials and observers to follow the procedures correctly and to notify the public of any possible violations. The Estonian National Electoral Committee (NEC) felt that although the observability of the electronic tally can be considered in the future, the effort needed to implement end-to-end verifiability is currently not justified.

Second, achieving some additional properties would have meant implementing a completely new system with a completely new user experience compared to what the electorate is used to, and this was considered unrealistic. As we will see later in the paper, cast-as-intended and recorded-as-cast properties are achievable incrementally with respect to the current system.

IV. Verifiable Internet voting for Estonian elections

In Estonia, Internet voting makes heavy use of an existing ID card infrastructure which essentially provides one secure pre-channel between the state and the citizen in the form of certified public-private key pairs.

Since verification is something that can only happen *after* a vote is cast, we also need a post-channel that would work well together with the chosen pre-channel. During the analysis phase, a postal+SMS solution was briefly considered. It was concluded that this channel was rather expensive and still error-prone as shown by the Norwegian experience [27]. Hence another alternative was needed.

Since the basic Estonian Internet voting protocol supports vote auditing by releasing the random seed used for encryption, we decided to implement this form of verification. Of course, such a verification cannot be performed by a human alone and a computing device is required. Since verification using the same device (PC) would not address the problem of potential device corruption, we decided to introduce verification on a different platform. As of the time of the development period (2012), the prime candidates for this platform were mobile devices (smartphones, tablet computers, etc.). They provide both sufficient processing power for cryptographic operations and independent communication channels.

Verification itself requires relatively small overhead compared to the existing Estonian Internet voting system, and the entire protocol on a high level is as follows (see also Figure 2).

1) The voter authenticates herself for the server.
2) She receives a list of candidates L.
3) The voter makes her choice $c_v \in L$ and prepares the vote $b_{anon} = Enc_{s_{pub}}(c_v, r)$, encrypted with the server's public key, using randomness r. The voter sends her signed vote $b = Sig_v(b_{anon})$ to the server.
4) The server returns a unique randomly generated vote reference vr to the voter. This reference will later be used to download the correct vote to the mobile device.
5) The voter transfers r and vr from the PC to the mobile device.
6) The mobile device contacts the server over server-side authenticated HTTPS and sends vr.
7) The voter's mobile device downloads the vote b_{anon} corresponding to vr from the server together with the list of all candidates available L.
8) The mobile device computes $Enc_{s_{pub}}(c, r)$ for all $c \in L$. If for some c' the equality $Enc_{s_{pub}}(c', r) = b_{anon}$ holds, this c' is displayed to the user. If $c_v = c'$, the voter accepts the vote to have been cast as intended.

Steps 1–3 have been used since 2005 and are familiar to the general electorate. Hence, only steps 4–8 are new to voters. From the user interface point of view they can be performed rather smoothly.

The time allowed to complete steps 4–7 has been limited (30 minutes in 2013 and 60 minutes in the 2014 elections). Also, the number of times the server is ready to let the user download b_{anon} is limited (currently 3). The verifiability extension only allows for the verification of the last vote cast by the voter. Re-

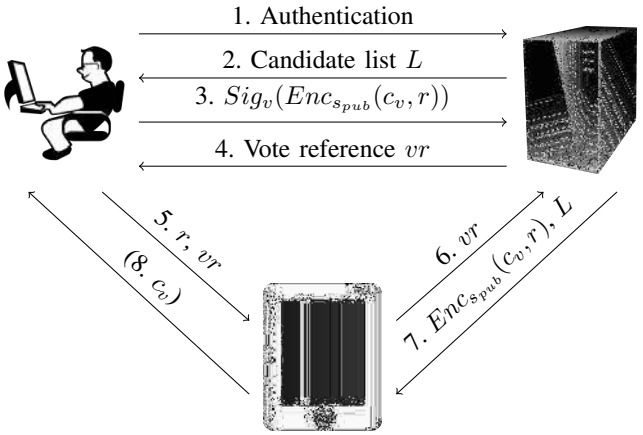


Fig. 2. The Estonian Internet voting protocol with vote verification

voting revokes both the previous ballot and the vote reference. These are largely anti-coercion measures; see Section V-B for further discussion.

The most complicated one is step 5, where the random seed r and vote reference vr need to be transferred from a PC to a mobile device. Several channels can be used for that; we chose to use QR codes, since other alternatives (like a memory card, a wired connection or Bluetooth) require extra setup. When the vote is sent to the server, a QR code containing r and vr is displayed on the PC screen. The user runs a verification application on the mobile device. The application first expects to scan the QR code, which can be done by pointing the device to the PC screen. The voter does not even need to press any buttons, as the scan is completed automatically. And assuming the network connection is open, steps 6 and 7 are also automatic. Once the vote is received from the server, the mobile device follows through with step 8.

Note that the mobile device never learns the voter's identity, it just sees random values. It finds the value c' for an anonymized encrypted vote. This prevents a malicious mobile device from breaking vote privacy. Of course, it can still lie about the value of c' found, but assuming that the PC and the mobile device are not corrupt in a coordinated manner, this lie would be detected and reported by the user with high probability. The latter assumption may or may not fully hold; see Sections V and VI for more discussion and analysis in case this assumption is relaxed.

Since step 8 assumes going through the list L, it will take some time. In practice, the candidate lists in Estonia contain up to several hundred elements in extreme cases (with the values $10 \ldots 50$ being the most common). We implemented a test application computing 400 RSA2048 encryptions with the exponent 65537. On a Samsung Galaxy Ace smartphone with an 800 MHz processor this computation took roughly 1.5 seconds. Together with the time needed to communicate with the server we estimate the total running time of the verification to be up to 5 seconds which we consider a reasonable result.

It would also be possible to implement step 8 by first asking the voter to input her choice and make the comparison with one encryption, displaying a simple yes/no answer. This

seemingly more elegant solution introduces a new potential threat vector. Namely, it would be possible for a corrupt verification application not to verify anything and just say yes. In the protocol proposed above, however, in order to manipulate the vote successfully without the voter noticing, the voting and verification applications must be corrupt in a coordinated manner. We consider the complexity of such an attack prohibitively high.

In principle, it is also possible to develop vote verification software for PC platforms and carry out a public education campaign convincing voters to verify their votes on a computer different from the one that they used to cast the vote. However, we suspect that the vast majority of voters would just run the two pieces of software on the same computer, and hence the security goals set for verification would not be achieved. At the time of writing this paper, major PC and mobile platforms are running different operating systems. Thus, the voters are forced to use separate devices for voting and verification which was one of our security goals. We acknowledge that this situation may change in the future, but at least for the elections taking place in 2013–2015 this approach should be viable.

Analyzing the voting protocol, we see that the verification device does not need and should not store anything. This means that these devices can be shared among voters, making them even more accessible.

V. Discussion

In this section we will address some specific issues about the scheme and its application.

A. Failed verifications

Individual verifiability provides NEC with an additional tool to detect possible attempts to manipulate the voting result on a large scale. Verification attempts may fail due to simple user errors or hardware/software incompatibility, but failed verifications may also indicate a manipulation attack.

Most important failures in verification can manifest themselves through the following symptoms:

- Inability to download the encrypted vote from the server,
- Failure to find the corresponding candidate from the list L,
- The candidate found does not match the voter's intention.

In case of such failures, NEC suggests that voters follow a predefined set of actions:

1) Re-vote and verify using (preferably) a different PC and mobile device.
2) In case the error persists, re-cast the vote in a polling station on paper. Notify NEC of the event.

If certain errors start repeating, this information may be used by NEC to initiate research activities and take different decisions. Failures in verification do not necessarily mean that an attack is going on. E.g. a voter who would attempt to verify her vote after the vote reference vr has expired, would get a verification failure. Similarly, a voter using the wrong QR-code would get a verification failure and possibly turn to NEC for assistance.

B. Coercion-resistance

Ben Adida, author of the verifiable Internet voting system Helios, states that his system is only suitable in low-coercion settings like student governments, local clubs, online groups such as open-source software communities, and other similar situations. The protocol is not applicable for parliamentary elections. for instance [5]. The original Helios interface actually provided a "Coerce Me!" button to remind the users about the inherent threat. A similar button could be built into the Estonian voting or verification application – anyone who gets hold of the vote $b_{anon} = Enc_{s_{pub}}(c_v, r)$ and randomness r is capable of finding out the voter's actual preference.

Coercion is more likely to occur in a remote setting. Voting in polling stations takes place in the privacy of the polling booth, and the coercer has to invent ways to maintain control over the actions of the coercee. In remote environments, the coercer can observe the voter voting for a specific candidate. Estonian Internet voting uses re-voting as an anti-coercion measure.

Verifiability seems to facilitate coercion. In the Norwegian system, the coercer may ask the voter to provide the card with the verification codes and the SMS with the code actually returned. This way the coercer can be sure that the vote for the required candidate is in the digital ballot box. In the Estonian protocol, it is enough for the coercer to control the verification application.

We argue that due to the option of re-voting, coercion is not made any easier by introducing verifiability. By observing either voting or verification, the coercer cannot be sure that the vote will actually be taken into account. We also note that a coercion attack as a manipulation attack is rather inefficient. In order to achieve an additional seat in the Parliament, a great number of people have to be coerced, and thus the probability of getting caught increases. It is also time-consuming to monitor all the coercees and their actions. (Recall that both the time the server is willing to provide a particular encrypted vote for verification, and the number of times it is ready to do so, are limited.) Nevertheless, if a society sees large-scale coercion as an existing problem, any kind of remote voting – electronic or non-electronic – should be avoided at elections.

C. The threat of false verification failure claims

Of course, introducing a new component into the system also brings along new attack vectors. Merely the possibility to claim that the verification failed can be misused by malicious voters interested in, say, a reputation attack [14]. When the proposed method of vote verification was presented to Estonian politicians, this was one of the concerns they expressed. The problem is that it is very difficult to either prove or disprove such claims without violating vote secrecy. The Norwegian experience, however, showed that a widespread reputation attack based on bogus claims did not happen [27]. On the contrary, the Norwegian electorate perceived failed verifications as a positive feature – it gave feedback that had been impossible to obtain before. After having applied the verification solution in the 2013 and 2014 Estonian elections we can say that the threat of false claims did not materialize. Considering that the

verifications made during the 2013 and 2014 elections were just pilots, the incentive of potential attackers may have been lower than for legally binding runs, and thus we still need to be ready for such an attack in the future.

D. Random factor exposure

The verification scheme leaks the randomness r used in the encryption to the mobile device. Anybody in possession of r, b_{anon} and the list of candidates L can brute-force the encrypted ballot to get the candidate number. We do not see a new threat here as anybody having access to r in the voting application also could have observed the original choice encrypted together with the randomness.

E. Diverting the verification

To provide its security properties, the verification protocol relies on some assumptions. The most important assumption made is the independence of the PC and the mobile device. If an attacker was able to install malware working on both of the devices in a coordinated manner, a potential vote manipulation could go unnoticed. The report [12] claims to have developed proof-of-concept pieces of malware for both the PC and the mobile device, using the QR code channel to make hints to the verification application about the voter's choice, whereas a compromised voting client would manipulate the vote silently.

However, the report fails to describe how to achieve a coordinated installation of the developed malware on these devices. The authors of the report also admit that if this attack were to be used on a large scale, it would carry an elevated possibility of detection, since some users may attempt verification with devices owned by others. This in turn means that the goal of introducing verification has been achieved and it is still possible to have confidence in the absence of a large-scale vote manipulation attack. See Section VI for more discussions on quantified estimates on the security guarantees obtained on the example of the 2013 Estonian elections.

Another approach to attack the scheme is based on the fact that the voter is not capable of verifying if the QR presented by the voting application contains the randomness and vote reference vr corresponding to her ballot. If the malicious voting application knows the vote reference vr_1 of an already stored ballot, which encrypted the candidate number desired by the voter, then the application could encrypt any other candidate number for vr, but show the QR code with vr_1 and r_1. This way a manipulated ballot would be stored, but the verification application would show the result expected by the voter.

The limits on the number and time of verifications and the way that the re-voting is handled make this attack difficult to execute in practice. It is not possible to acquire a set of QR codes and reuse them for a longer period of time. A more robust approach would be based on the fact that most votes are never verified and it is possible to build a QR-sharing bot-net of malicious voting applications. This would make the setup of a manipulation attack more complex, and the event of using the same QR code too many times would trigger a server-side alarm.

Vote verification is not a universal measure against all possible attacks. As discussed above, re-voting is used in Estonia as an anti-coercion measure. However, this possibility can also be abused by malware installed on the voter's PC. During the original voting session, the malware may save the PIN codes of an ID card (assuming an ID card reader without a PIN pad is used, which is mostly the case). If the ID card is inserted again later (maybe for a completely different application), the malware may also use it to submit a new vote. As there is no active feedback channel currently in use in the Estonian Internet voting protocol, most voters would never know about this occurrence even if they verified their original vote. The most efficient measure against such an attack would be to implement an active feedback channel. This is one of the possible future improvements considered for the Estonian Internet voting protocol. However, since this attack is independent of verification, further discussion remains outside the scope of the current paper.

VI. Implementation results

The described verifiable Internet voting system was first implemented for the 2013 Estonian local municipal elections. For the first pilot[1], only Android OS 2.2 and higher were supported as the mobile application platform. During the elections, 136,853 electronic votes were given (including re-votes) and 133,662 counted (which comprised 21.2% of all the votes cast). Verification was utilized on 4,696 occasions (and altogether 3.43% of all the e-votes given were verified).

For the second pilot run during the 2014 European Parliament elections, support for iOS and Windows Phone was added as well. During the elections, 105,170 electronic votes were given (including re-votes) and 103,105 votes were counted (which comprised 31.3% of all the votes cast). Verification was utilized on 4,250 occasions (and altogether 4.04% of all the e-votes given were verified).

There were no failed verifications reported in 2013. This allows us to estimate the probability that a large-scale vote manipulation went undetected. Assuming that the attacker was able to manipulate k random votes, but not tamper with the verification devices and voting devices in a coordinated manner, the probability that at least one of the manipulated votes was detected is

$$1 - \left(1 - \frac{4696}{136853}\right)^k .$$

(This corresponds well to the reasoning by Neff [21].)

In order to obtain a more realistic estimate on this probability, we have to take into account possible coordinated malware (see Section V). For illustrative purposes in this paper we assume that only half of the verifications were performed on truly independent devices. The probability that at least one of

[1]According to the current Estonian legislation, verification will have legal consequences in 2015 (and the date can be moved further if necessary). The verifications during the first two elections of 2013 and 2014 were planned as pilots to try out the new technology.

the manipulated votes was detected changes to

$$1 - \left(1 - \frac{2348}{136853}\right)^k .$$

See Figure 3 which depicts both of the graphs. We can see that even if half of the devices were compromised, the manipulation of 200 or more votes would still be detected with more than a 95% probability.

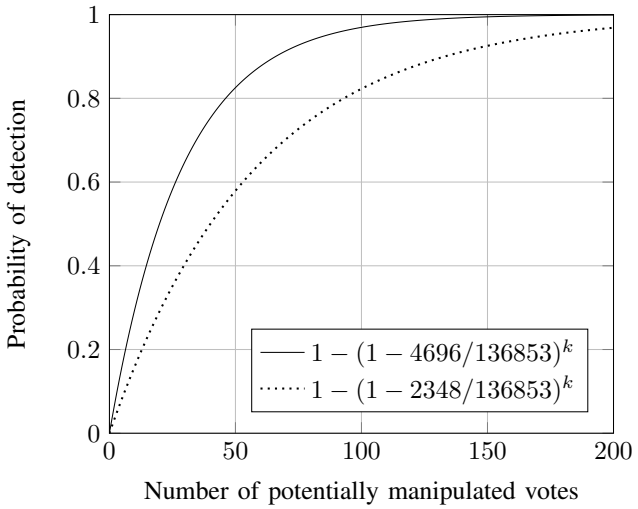


Fig. 3. Probability of large scale vote manipulation detection

The pilot in 2014 was more controversial – during the election, two software bugs were discovered in the iOS verification application. On a few occasions, the iOS application reported that it was not capable of finding the candidate number corresponding to the encrypted ballot. It appeared that binary data extracted from the QR code was interpreted as a string by the application, leading to bad encryptions under certain circumstances. The bug was fixed during the elections, the patch was successfully submitted to the iOS app store and pushed to the voters.

The second bug manifested itself when a buggy iOS verification application was accidentally used with a QR code coming from an external source (e.g. newspaper ad, online media, etc.). For the voter it looked as if her vote was not available on the server, even though it was stored correctly. This resulted in four calls to the helpdesk. The voters were instructed to cast a new vote and verify it again. No more errors were reported after this.

Hence no real vote manipulations were detected during the 2014 elections either. This allows us to estimate the probability of a large-scale attack detection exactly the same way as was done for the 2013 elections above.

VII. Conclusions and further work

In this paper, we described an extension to the Estonian Internet voting protocol, allowing users to verify that their votes are stored correctly on the server. We discussed the technical aspects and quantified the resulting security guarantees obtained during two pilot application runs.

On the one hand, Estonian democracy is rather young and all the potential weaknesses of Internet voting are aggressively used in political battles to attempt revocation or at least harm the reputation of this voting method. On the other hand, Estonian society is also very technology-oriented. For example, virtually all the eligible voters have a digital ID card capable of giving legally binding RSA signatures, and the penetration of mobile devices is growing rapidly. These considerations allowed us to propose a verifiable Internet voting scheme relying on an ID card as a pre-channel and a mobile device as a post-channel. In order to successfully and non-discoverably manipulate a vote, the attacker has to corrupt both the voter's PC and mobile device in a coordinated manner. Even if this is conceivable for a small number of votes, we consider the complexity of a corresponding successful widespread attack prohibitively high.

The system was implemented as a pilot solution for the 2013 Estonian local municipal elections and the 2014 European Parliament elections. It is expected to have legal implications in the 2015 parliamentary elections. Before legally binding conclusions can be drawn, new dispute resolution mechanisms need to be created. For example, we need to better understand how to distinguish true verification failure claims from false ones and how to deal with these false claims.

The success of the proposed system relies on the fact that currently PCs and mobile devices are independent and run different operating systems. This situation may change in the future, which means that the system will then need to be modified suitably. Also, the first pilot implementations of 2013 and 2014 are expected to give a lot of feedback, and improving the system accordingly will remain the subject of future development efforts.

Acknowledgements

This research was supported by the Estonian Research Council under Institutional Research Grant IUT27-1 and the European Regional Development Fund through the Centre of Excellence in Computer Science (EXCS) and grant project number 3.2.1201.13-0018 "Verifiable Internet Voting – Event Analysis and Social Impact".

The authors would also like to thank Arnis Paršovs for proofreading the paper and all the anonymous reviewers for their excellent comments.

References

[1] Forschungsgruppe Internetwahlen, Zweiter Zwischenbericht zum Projekt, Strategische Initiative:WahlenimInternet'nachAbschlussderWahlenzum Studierendenparlament der Universität Osnabrück am 2. Feb. 2000, 2000.

[2] Report of the National Workshop on Internet Voting: Issues and Research Agenda. Internet Policy Institute, http://verifiedvoting.org/downloads/NSFInternetVotingReport.pdf, 2001, last accessed May 6th, 2014.

[3] Legal, operational and technical standards for e-voting. http://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf, April 2005, last accessed May 6th, 2014. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum.

[4] The Geneva Internet Voting System. http://www.geneve.ch/evoting/english/doc/final-livret-anglais.pdf, last accessed May 6th, 2014.

[5] Ben Adida. Helios: web-based open-audit voting. In *Proceedings of the 17th conference on Security symposium*, pages 335–348, 2008.

[6] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, WPES '06, pages 29–40, 2006.

[7] Jordi Barrat, Michel Chevallier, Ben Goldsmith, David Jandura, John Turner, and Rakesh Sharma. Internet Voting and Individual Verifiability: The Norwegian Return Codes. In Melanie Volkamer Manuel J. Kripp and Rdiger Grimm, editors, *5th International Conference on Electronic Voting 2012 (EVOTE2012)*, volume 205 of *LNI – Lecture Notes in Informatics*, pages 35–45, 2012.

[8] Christian Bull and Henrik Nore. Problems encountered. Seminar on Internet voting, http://www.regjeringen.no/pages/38377245/5_problems_encountered.pdf, September 2013, last accessed May 6th, 2014.

[9] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *Proceedings of the conference on Electronic voting technology*, EVT'08, 2008.

[10] Andreas Ehringfeld, Larissa Naber, Karin Kappel, Gerald Fischer, Elmar Pichl, and Thomas Grechenig. Learning from a Distributed Denial of Service Attack against a Legally Binding Electronic Election: Scenario, Operational Experience, Legal Consequences. In Kim Andersen, Enrico Francesconi, ke Grnlund, and Tom van Engers, editors, *Electronic Government and the Information Systems Perspective*, volume 6866 of *Lecture Notes in Computer Science*, pages 56–67. Springer Berlin / Heidelberg, 2011.

[11] Kristian Gjøsteen. Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380, 2010. http://eprint.iacr.org/.

[12] J. Alex Halderman, Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer, and Drew Springall. Security Analysis of the Estonian Internet Voting System, May 2014. https://estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf.

[13] Sven Heiberg, Peeter Laud, and Jan Willemson. The Application of I-voting for Estonian Parliamentary Elections of 2011. In Aggelos Kiyaias and Helger Lipmaa, editors, *VoteID 2011*, volume 7187 of *LNCS*, pages 208–223. Springer, 2011.

[14] Sven Heiberg and Jan Willemson. Modeling threats of a voting method. In Dimitrios Zissis and Dimitrios Lekkas, editors, *Design, Development, and Use of Secure Electronic Voting Systems*, pages 128–148. IGI Global, 2014.

[15] E.M.G.M. Hubbers, B.P.F. Jacobs, and W. Pieters. RIES: Internet voting in action. In *29th Annual International Computer Software and Applications Conference (COMPSAC 2005)*, pages 417–424. IEEE Computer Society, 2005.

[16] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), 2004, last accessed May 6th, 2014. http://www.servesecurityreport.org/paper.pdf.

[17] Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira. Veryvote: A voter verifiable code voting system. In Peter Y. A. Ryan and Berry Schoenmakers, editors, *VOTE-ID*, volume 5767 of *Lecture Notes in Computer Science*, pages 106–121. Springer, 2009.

[18] Robert Krimmer, Andreas Ehringfeld, and Markus Traxl. The Use of E-Voting in the Austrian Federation of Students Elections 2009. In Rober Krimmer and Rüdiger Grimm, editors, *4th International Conference on Electronic Voting 2010*, Lecture Notes in Informatics, pages 33–44, 2010.

[19] Lucie Langer, Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. Classifying Privacy and Verifiability Requirements for Electronic Voting. In *GI Jahrestagung*, pages 1837–1846, 2009.

[20] Ülle Madise and Tarvi Martens. E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In Robert Krimmer, editor, *Electronic Voting 2006, Proceedings of the 2nd International Workshop*, LNI GI Series, pages 15–26, 2006.

[21] C Andrew Neff. Election confidence, 2003, last accessed May 6th, 2014. http://www.verifiedvoting.org/wp-content/uploads/downloads/20031217.neff.electionconfidence.pdf.

[22] OSCE/ODIHR. Estonia. Parliamentary Elections 6 March 2011. OSCE/ODIHR Election Assessment Mission Report. http://www.osce.org/odihr/77557, 2011, last accessed May 6th, 2014.

[23] Stefan Popoveniuc, John Kelsey, Andrew Regenscheid, and Poorvi Vora. Performance requirements for end-to-end verifiable elections. In *Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections*, EVT/WOTE'10, 2010.

[24] Caltech-MIT Voting Technology Project. Voting: What is, what could be. Technical report, Caltech/MIT, 2001.

[25] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

[26] Gerhard Skagestein, Are Vegard Haug, Einar Nødtvedt, and Judith E. Y. Rossebø. How to create trust in electronic voting over an untrusted platform. In Robert Krimmer, editor, *Electronic Voting*, volume 86 of *LNI*, pages 107–116. GI, 2006.

[27] Ida Sofie Gebhardt Stenerud and Christian Bull. When Reality Comes Knocking. Norwegian Experiences with Verifiable Electronic Voting. In Manuel Kripp, Melaine Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting 2012*, Lecture Notes in Informatics, pages 21–33, 2012.

Experiences with Voting Machines

From Piloting to Roll-out: Voting Experience and Trust in the First Full e-election in Argentina

Julia Pomares
Political Institutions Program
Center for the Implementation of Public Policies Promoting Equity and Growth
Buenos Aires, Argentina
jpomares@cippec.org

Ines Levin
Department of Political Science
University of Georgia
Athens, United States

R. Michael Alvarez
Division of the Humanities and Social Sciences
California Institute of Technology
Pasadena, United States

Guillermo Lopez Mirau
Under-Secretariat for Planning of the Government of the province of Salta
Salta, Argentina

Teresa Ovejero
Electoral Secretariat
Electoral Tribunal of the province of Salta
Salta, Argentina

***Abstract*— Despite the conventional wisdom that e-voting would take place first in established democracies and later in developing countries, the speed of implementation has been higher in the developing world, especially in Latin America, with several countries such as Brazil, Venezuela, Argentina and Ecuador implementing e-voting methods. This paper looks at the experience of Salta, the first Argentine district rolling out e-voting for the entire electorate in 2013. Based on a survey of 1,000 voters in the 2013 provincial elections, the voter's experience and confidence in the election process is analyzed. Among the key findings, there is a strong effect of a voter's ability to use the voting machine without assistance on the overall support for e-voting and positive perceptions of integrity in the election process. These results have both theoretical and policy implications.**

Keywords*— *e-voting; confidence; usability; Latin America; Argentina

I. INTRODUCTION

In the 2013 elections, Salta became the first province in Argentina to implement an e-voting system for the entire electorate (about 900,000 voters). The system was used to select provincial candidates – there are compulsory primaries for voters and parties[1] – and to elect provincial legislators and council members in the municipalities throughout the province. The election took place amidst a wave of change in voting procedures at the provincial level in Argentina [1] [2] [3] [4]. Although national elections are still conducted using the ballot and envelope system (also called French system by which each party is responsible for printing and disseminating ballots), several provinces including some of the most populated ones – the autonomous City of Buenos Aires, Santa Fe, and Cordoba – have changed legislation to introduce new voting procedures. Against this background, lessons learnt from Salta – one of the few districts[2] of the country with an important proportion of indigenous people[3] – are key to informing other provinces as well as other countries in the region seeking to implement e-voting systems. For example, Ecuador has piloted the same system used in Salta in the 2014 local elections.[4]

Based on a survey of 1,000 voters conducted on Election Day (November 10, 2013), this paper analyzes two central aspects of voters' attitudes toward the voting system:

[1] Since 2009, all legislative and executive candidates must be nominated through primaries. Parties must hold primary elections, even if there is no internal competition. Candidates need to get 1.5% of votes in the primaries in order to get to the general stage. Participation in primaries (and general elections) is compulsory.

[2] Each of the 24 provinces serves as an electoral district for the national Senate and chamber of deputies.

[3] According to the last National Census (2010), 2.7% of Argentine population are indigenous. The highest proportions are to be found in four provinces, including Salta (8% of the population).

[4] See Consejo Nacional Electoral, "Simulacros de voto electrónico probarán eficacia del sistema," http://www.cne.gob.ec/index.php/Boletines-de-prensa/Articulos/simulacros-de-voto-electronico-probaran-eficacia-del-sistema.html.

perceptions and opinions about the voting experience, with a special focus on the use of the voting machine, and perceptions about the integrity of the electoral process. The paper is structured as follows. Section 2 presents our motivation for the analysis of these attitudes and the questions of the survey. Section 3 goes into detail about how e-voting is being implemented in Argentina and the context of the 2013 election under analysis. Section 4 presents the data and results of a statistical analysis of the determinants of voting experience and confidence in the integrity of the electoral process. Section 5 concludes by focusing on the policy implications of the key findings.

II. WHY FOCUS ON VOTERS' EXPERIENCES AND PERCEPTIONS OF ELECTORAL INTEGRITY?

Our interest in the voting experience is justified by the fact that voting technologies frame the voting experience in direct and indirect ways. Directly, the voting experience might affect the degree of satisfaction that people draw from that experience and opinions about the change in voting procedures. Indirectly, it might influence opinions about the transparency and integrity of elections. Also, in the context of a very diverse population, we are interested in understanding the socio-demographic determinants of evaluations of the voting system. Do differences in age and education affect voter evaluations? Does living in the urban Capital affect perceptions of ease of use and overall assessments of the new voting system? In order to answer these questions, we look at perceptions of usability and speed of the voting procedure, opinions about ease of use of different interactions with the voting machine (inserting the ballot, operating the touchscreen device and finding the candidates), as well as overall evaluations of the new voting system.

Second, we focus on confidence in elections for both theoretical and policy reasons. On the one hand, an increasing body of literature looks at trust in voting technologies in both established [5] [6] [7] [8] and developing democracies [9] [10] [11]; [12]; [13] [14]. Whereas quantitative analyses follow an inductive approach and test whether individual- or institutional-level variables shape perceptions of trust, qualitative accounts look at the *socio-cultural aspects* of the election process that are shaped by voting procedures [15]. Following previous research of the authors [1] [4], this paper places key importance on breaking down the concept of confidence into different dimensions, differentiating between perceptions of accuracy and secrecy.

At the same time, studies of trust in elections also have important policy implications. The increasing interest in e-voting technologies in developing countries is usually associated with trying to building confidence in the fairness of the electoral process. Studies of elections in Latin America [1] [16], as well as comparative studies [17], show that the focus on boosting perceptions of trust in electoral processes is an important driver of the move toward electronic voting technologies. Against this background, the Salta election is of key policy relevance since this first full implementation of e-voting might shed light on the potential consequences of introducing e-voting in other developing countries, many of which are already testing and deploying new voting procedures (such as Mexico, Ecuador and Peru).

Three questions on confidence in the election were asked. First, we distinguished between two specific dimensions of confidence in the election process: confidence that a vote will be counted as intended and confidence that the ballot will be kept secret. Whereas the former assesses perceptions of accuracy of the voting system and fairness of the counting procedure, the latter captures the ability to preclude violations of privacy and voter intimidation. Additionally, we looked at broader perceptions of the cleanness of the election.

III. E-VOTING IN ARGENTINA

The voting system traditionally used throughout the country in Argentina is the French system of ballot and envelope. Typically, a paper ballot contains party-specific candidates for multiple races that take place on the same day – which might include candidates to the presidency, national deputies, governor, provincial deputies, mayor, and local councils – and dotted lines indicate to voters how to split their vote across down-ticket races. On Election Day, voters vote in private (i.e. behind closed doors) inside a room denominated "*cuarto oscuro*" where party-specific paper ballots are displayed on several tables. Once inside the room and on their own, voters select their favorite candidates for each race – they can split their vote by picking parts of party-specific ballots, or they can vote straight-ticket by picking an unbroken party-specific ballot – and place their choices inside an envelope that they subsequently insert into a ballot box located outside the "*cuarto oscuro*."

Another important feature of the traditional voting system is that each party is responsible for printing the ballots, as used to be case in the first applications of the French system in the United States.[5] This means that once ballots are displayed in voting booths, parties are responsible for guaranteeing their supply throughout Election Day. This was not a problem under the historic two-party system in Argentina, but has increasingly come into question with the rise in political fragmentation since 1999. On the occasion of the 2007 national legislative elections, for instance, there were several claims of ballot manipulation in the province of Buenos Aires, the largest district of the country. As a consequence, the National Electoral Chamber – the highest electoral court – called for changes to the voting procedure to guarantee that all electoral options are made available to voters.

In recent years, several provinces have introduced reforms to their electoral processes, including the adoption of e-voting and of different types of the Australian ballot.[6] Salta, a province located in the northwestern part of the

[5] For a detailed analysis of the implementation of the Australian ballot in American elections, see [18].

[6] By Australian ballot, we refer to the system in which all parties are on the same official ballot, provided by the electoral authority and the voter marks her option.

country with electoral roll of about 900,000 voters, became the first province to introduce an e-voting system for general provincial elections in 2009. E-voting machines used in Salta allow voters to select candidates electronically using a touchscreen, and subsequently print choices on paper ballots that voters deposit in a ballot box. At the close of the polls, the voting machines turn into tallying machines that poll workers use to count votes. Under this new system, the relatively private act of selecting electoral options behind doors inside a "*cuarto oscuro*" is replaced with a much more public act, using a machine within sight of other voters. Although voting machines are placed inside the polling place using a layout that seeks to preserve voter privacy, the abandonment of the "*cuarto oscuro*" might induce negative perceptions of vote secrecy [3] [4].[7]

The electronic voting system was first tested in 2009 during the primaries of the Peronist party at selected polling stations in the capital of the province and suburbs. In 2011, the e-voting system was used during the primary and general elections, when the roll-out was extended to 33 per cent of the province's electoral roll. The gradual implementation of e-voting in Salta allowed researchers to learn about the impact of e-voting by comparing the voting experiences of first-time e-voters and voters who continued using the traditional voting system [3] [4]. Although the government plan was to implement the e-voting system in two more subsequent stages (66 per cent of voters in 2013 and full roll out in 2015), the provincial Executive decided to fully implement the electronic system in 2013, extending it to the entire electoral roll. In this paper, we study the impact of voting experiences on attitudes toward the e-voting system among first- and second-time e-voters, using data from a voters' survey conducted during the 2013 general election in Salta.

In 2013, the e-voting system was implemented for the whole electorate (892,000 voters in 2700 polling tables) first for compulsory open primaries (6 October) and several weeks later (10 November) for the general provincial elections. Some comments about the political context of the election are necessary. A very negative electoral campaign took place in this midterm election and the incumbents did not perform well. Whereas the governor got reelected in 2011 with 60 per cent of the votes (when e-voting was piloted for one third of the electorate), his legislative candidates got only 20 per cent of the votes in the 2013 contest. Also, it is important to add that the main opposition to the governor throughout the province came from a faction of the incumbent Peronist Party. Although these political leaders supported the change in voting procedures in 2011, they strongly opposed it in 2013. Moreover, the debate about the roll out of the e-voting system played a key role in the electoral campaign. The main provincial newspaper (*El Tribuno*) dedicated the front pages of the paper in the last week of the election to the prospect of e-voting machines functioning properly on Election Day. It was a very competitive election, especially in the Capital City. For the first time in their history, the Workers' Party (of left-wing ideology) got the first place in the election in the Capital of the province with 27 per cent of the votes.

In order to grasp the perceptions of voters and poll workers about the e-voting system, the Electoral Tribunal (part of the Judiciary), the Executive government and the Buenos Aires-based think tank CIPPEC designed and conducted a survey of 1,000 voters and 185 poll workers. Both surveys were administered on Election Day. This paper presents the results of the voters' survey, focusing on two central issues: the voting experience, and different dimensions of voter's confidence in the election process and evaluations of the voting system.

A stratified sample of 24 schools (polling stations) throughout the province was created. In all, nine municipalities were selected including the provincial Capital (concentrating 60 per cent of the provincial electorate and where most e-voting piloting took place in 2011). A team of two pollsters was assigned to each polling station. Each pollster was expected to administer at least 20 voter surveys. They were told to randomly recruit voters on their way out of the polling tables. In order to ensure a uniform socio-demographic distribution of the sample, half of their surveys had to be administered to men and they also had to follow age quotas. We present findings from the data in the next section.

IV. Voting Experience and Perpceptions of Integrity during the 2013 Elections

A. A first look at the data

When asked about perceptions of ease of use and speed of the voting system, we find very positive responses among Salta voters: 9 out of 10 voters said that voting was *very* or *somewhat* easy, and 8 out of 10 said that voting was *fast* or *very fast* (Table I). Voter opinions are also overwhelmingly positive when surveyed about the ease of interacting wit different features of the voting machine: approximately 9 out of 10 said instructions were easy to understand, and a similar number said that inserting the ballot into the machine, using the touchscreen and finding the voting option was easy (Table I). Also, voters reported very positive opinions about the qualification of poll workers: 72 per cent said that they were *very* or *somewhat* qualified to exercise their roles.

TABLE I: Perceptions of Ease of Use and Speed of Voting Procedure

Ease of Use and Speed of Voting Procedure	%
Voting was easy	88.7
Voting was fast	80.3
Machine Ease of Use	%
Instructions were easy to understand	92.3
Inserting the e-voting ballot was easy	87.5
Using the touchscreen was easy	91.3
Finding the voting option was easy	88.8

Note: summary statistics were computed excluding non-responses (N=981).

[7] Interested readers can find more description of these voting systems, and photographs of the voting devices in [3] [4].

Despite these positive evaluations of the voting experience, 1 out of 5 voters said that they experienced a problem while voting and 13 per cent of voters needed help in order to be able to cast a ballot (Table II). There are significant differences by age and education. The proportion of voters needing help doubles among least educated voters: 27 per cent of those with no formal education or only primary education needed assistance. Also, voters older than 50 years experienced more difficulties: 23 per cent of them reported having asked for help. Demanding assistance to understand the voting system is an important consideration because if poll workers are unable to help voters and preserve privacy at the same time, the secrecy of the ballot might be called into question.

TABLE II: Responses to questions about Voting Experience

Other Aspects of Voting Experience	%
Experienced a problem while voting	19.0
Thinks electoral authorities were qualified	72.2
Needed help while voting	13.1
Voter chose to split his/her ticket	34.4

Note: summary statistics were computed excluding non-responses (N=981).

Interesting insights also come out of questions inquiring about general evaluations of the system: an overwhelming majority evaluates the system in positive terms. When asked "in broad terms, how would you evaluate the voting system used today," 8 out of 10 voters said *very good* or *good*. Despite these positive opinions, a majority of voters (53 per cent) said that they would like to switch back to the traditional paper ballot system.

TABLE III: General Evaluations of the System and Voter confidence

General Evaluation of e-voting System	%
Evaluated system in positive terms	82.0
Prefers the traditional voting system	53.2
Confidence in the Election Process	%
Confident vote was correctly recorded	75.5
Confident in ballot secrecy	57.6
Believe elections in Salta are clean	35.0

Note: summary statistics were computed excluding non-responses (N=981).

Similar to previous findings on the 2011 elections, we find support for the hypothesis that perceptions of accuracy and secrecy operate differently: whereas there are high levels of trust in the ability of the system to correctly record the preferences of voters, with 75 per cent of voters reporting positive responses, voters seem more hesitant about ballot secrecy, with only 58 per cent reporting positive responses (Table III). The third question on perceptions of cleanness of the election got quite negative results: only 35 per cent of voters believe elections in Salta are clean. It is important to keep in mind that this question might capture a broader discontent with political parties and disaffection and not exclusively opinions about the voting system.

B. Statistical analysis

In order to gain a deeper understanding of the determinants of voter evaluations of the voting experience and confidence in the electoral process, we estimated a series of logistic regressions for a set of outcome variables related to: (a) voters' evaluations of ease of use and speed of the voting system; and (b) voters' confidence that their vote was recorded correctly and that ballot secrecy was preserved, together with general evaluations of the cleanness of elections in Salta. We included a set of control variables: encountering a problem while voting; perceptions of qualification of poll workers; having needed help while voting; having used the e-voting system in a previous election; whether the voter split his/her ticket; living in the Capital of Salta; age; gender; political information;[8] technology use; belief that technology simplifies life; and education.[9]

Tables IV through VII present estimates of marginal effects (i.e. changes in predicted probabilities that the binary dependent variable takes value one as a result of marginal changes in explanatory variables) and 95% confidence intervals. Results are presented in different tables based on the type of outcome variable: general evaluations of ease of use and speed of voting procedure (Table IV); ease of use of different features of the e-voting system (Table V); general evaluations of the e-voting system and preference for the previous ballot and envelope system – referred to here as "traditional voting" (Table VI); and, finally, voters' confidence in their vote being counted as intended, in ballot secrecy, and perceptions of the cleanness of elections in Salta (Table VII).

Looking at the determinants of perceptions of ease of use and speed of the voting procedure, we find a clear influence of asking for help and encountering a problem while voting, in the expected direction: asking for assistance reduces the probability of positively evaluating ease of voting by 13 percentage points. Also, encountering a problem reduces the probability of saying that voting was fast by 14.5 percentage points. Having used e-voting in the past also increases the probability of saying that voting was fast by 6 percentage points. An influence of age is also evidenced in these results: voters older than 49 years have a 3-point higher probability of saying that voting was easy. Interestingly, there is no effect of educational attainment on these perceptions (Table IV). At the same time, a strong belief in the benefits of technology (that is, strongly agreeing that technology makes life simpler) also increases the probability of holding positive perceptions of ease of use. Finally, more favorable evaluations of poll worker qualifications also have a positive influence on opinions about ease of use and speed of the voting procedure.

[8] Political information was computed as the number of correct answers among three questions measuring knowledge of persons holding salient positions in national and provincial governments.

[9] Missing values in dependent and explanatory variables were imputed using the R package *mice* [19] before estimating the regression models.

The two most direct measures of usability (encountering a problem while voting and asking for help) have considerable effects on saying that diverse actions were easily performed (Table V), including understanding instructions, inserting the ballot in the voting machine, using the touchscreen, and finding the preferred electoral option. For instance, asking for help reduces the probability of saying that inserting the ballot into the machine was easy by 20 percentage points. It is important to bear in mind that several problems had taken place during the voting process in the primary election conducted in October.[10]

Although it might be expected that experiences such as encountering a problem while voting and needing to ask for help influence perceptions of usability, it is less clear that they might affect overall evaluations of the system. We find, however, strong evidence that this is the case: asking for help increases by 15 percentage points the probability of preferring a return to the traditional means of voting with paper ballots. Perhaps not so surprisingly, those more likely to use technology in their everyday lives are less likely to prefer the old method of voting (Table VI). Voter evaluations of poll worker qualifications are also drivers of support for returning to the previous voting system. These results point to the importance of voting experience and usability issues for general evaluations of the e-voting system.

Finally, important findings can be drawn from the analysis of the determinants of confidence in the electoral process (Table VII). In line with results found for overall evaluations of the voting system, encountering a problem while voting is an important driver of negative perceptions of ballot secrecy (although not of perceptions of accuracy of the voting system). Quite remarkably, perceptions of qualification of poll workers are a strong determinant of voters' confidence in the integrity of the electoral process (favorable evaluations lead to 16.6 and 23.3 percentage point increases in perceptions of accuracy and secrecy of the voting process, respectively). Not only do these evaluations have an influence on specific dimensions of confidence in the voting process (accuracy and secrecy) but also exert considerable impact on thinking that elections in Salta are clean (a 22.1 percentage point increase). Also, after controlling for other factors, neither age, education, nor gender influence perceptions of confidence in the integrity of the electoral process. Only one demographic attribute exerts a statistically significant influence on voter confidence: living in the Capital vis-à-vis the interior of the province. Those living in the most urban areas are less likely to hold positive opinions on the secrecy of the ballot and are also less likely to believe that elections in Salta are clean. Lastly, the fact that those with more political information hold more negative opinions might indicate that negative reports about e-voting in the news media negatively influenced voters' perceptions.

V. Concluding Remarks

This paper has analyzed survey data from an important implementation of e-voting in Salta, Argentina. The primary focus has been on voter evaluations of the usability of the electronic voting system, and voter confidence in the electoral process. Since one of the main reasons for the move toward to electronic voting systems in Latin America is to improve voter perceptions of the integrity of the electoral process, it is important to evaluate voter reactions to these new means of ballot marking, casting and tabulation.

We find important results. In particular, we can conclude that voter confidence is associated with both the usability of the voting system and with the qualifications of those who assist voters when they have trouble with the system – poll workers. Both of these results shed light on dimensions of voter confidence that have not been well studied so far in the literature. Future research on evaluating new voting systems, and on voter confidence, needs to pay more attention to contextual determinants of confidence in the voting system and its integrity.

Finally, this paper has significant policy ramifications for nations in Latin America considering the adoption of new voting technologies. On one hand, the implementation of new voting systems – if accomplished with secure and usable voting technologies – may be able to improve voter confidence in the integrity of a nation's electoral process. New voting technologies, if well designed to address existing concerns with the traditional voting process, can help mitigate previous apprehensions. On the other hand, it is also seems clear that new voting systems can raise other concerns, for example, regarding voter privacy. Additionally, results discussed in this paper point to the importance of poll worker training: their job has key implications for voters' evaluations of the new system. It is only by adopting a scientific program evaluation – like that used in the recent implementations of e-voting in Salta – that the effects of adopting a new voting system can be measured and assessed.

Acknowledgements

We would like to thank the Voting Technology Project (CALTECH/MIT), Micromata, and Charles Stewart for their support to present this work at the EVOTE 2014.

[10] In the context of the primary elections, the media reported numerous cases of machines with problems reading ballots. According to informal talks with the provider, these problems were largely reduced for the general elections.

REFERENCES

[1] Alvarez, R. Michael, Ines Levin, Julia Pomares and Marcelo Leiras.. Voting Made Safe and Easy: The Impact of e-voting on Citizen Perceptions. Political Science Research and Methods 1(1), 2013, pp. 117-137.

[2] Katz, Gabriel, R. Michael Alvarez, Ernesto Calvo, Marcelo Escolar, and Julia Pomares. Assessing the Impact of Alternative Voting Technologies on Multi-Party Elections: Design Features, Heuristic Processing and Voter Choice. Political Behavior 33(2), 2011, pp. 247-270.

[3] Lopez Mirau, Guillermo, Teresa Ovejero, Julia Pomares. The Implementation of E-voting in Latin America: The Experience of Salta, Argentina from a Practitioner´s Perspective. Proceedings of the 5th International Conference on Electronic Voting 2012, Kripp, M.; Volkamer, M.; Grimm, R., Eds. Bregenz, Austria, July 2012.

[4] Pomares, Julia, Ines Levin, and R. Michael Alvarez. Do Voters and Poll Workers Differ in their Attitudes Toward e-voting? Evidence From the First e-election in Salta, Argentina. USENIX Journal of Election Technology and Systems 2(2), 2014, pp. 1-10.

[5] Alvarez, R. Michael, Thad E. Hall, and Morgan H. Llewellyn. 2008. Are Americans Confident their Ballots are Counted? Journal of Politics 70(3):754–66.

[6] Delwit, Pascal, Erol Kulahci, and Jean-Benoit Pilet. 2005. Electronic Voting in Belgium: A Legitimized Choice? Politics 25(3):153–64.

[7] Stewart III, Charles. Election Technology and the Voting Experience in 2008. Caltech/MIT Voting Technology Project Working Paper #71, http://www.vote.caltech.edu/sites/default/files/ElectionTechnology_CStewart_033109.pdf. 2009.

[8] Atkeson, Lonna Rae and Kyle L. Saunders. The Effect of Election Administration on Voter Confidence: A Local Matter? PS: Political Scince & Politics 40(4): 2007, pp. 655-660.

[9] Alvarez, R. Michael, Gabriel Katz, Ricardo Llamosa, Hugo E. Martinez.. Assessing Voters' Attitudes towards Electronic Voting in Latin America: Evidence from Colombia's 2007 E-Voting Pilot. E-Voting and Identity: Lecture Notes in Computer Science Volume 5767, 2009, pp 75-91.

[10] Alvarez, R. Michael and Thad E. Hall. Electronic Elections: The Perils and Promises of Digital Democracy. Princeton: Princeton University Press. 2010.

[11] Alvarez, R. Michael, Gabriel Katz, and Julia Pomares. The Impact of New Technologies on Voter Confidence in Latin America: Evidence from E-Voting Experiments in Argentina and Colombia. Journal of Information Technology & Politics. Volume 8, Issue 2. 2011.

[12] Fujiwara, Thomas. Voting Technology, Political Responsiveness, and Infant Health: Evidence from Brazil. Unpublished Manuscript. https://www.gsb.stanford.edu/sites/default/files/documents/pe_02_11_pefujiwara.pdf. 2010.

[13] Hidalgo, F. Daniel. Digital Democratization: Suffrage Expansion and the Decline of Political Machines in Brazil. Unpublished Manuscript. http://politics.as.nyu.edu/docs/IO/17524/hidalgo.pdf. 2010

[14] McCoy, Jennifer. One Act in an Unfinished Drama. Journal of Democracy 16(1): 2005.

[15] Dompnier, Nathalie. "Les machines à voter à l'essai. Notes sur le mythe de la "modernisation démocratique"." *Genèses (Genèses)*:, pp. 69-88.

[16] Rodrigues-Filho, Jose, Cynthia J. Alexander, and Luciano C. Batista. 2006. E-voting in Brazil—The Risks to Democracy. In Electronic Voting 2006, edited by. R. Krimmer & R. Grimm, 85–94. Bonn, Germany: Gesellschaft fur Informatik.

[17] Pomares, Julia. 'Inside the Black Ballot Box. Origins and Consequences of Introducing Electronic Voting Methods'. PhD diss., London School of Economics and Political Science. 2012

[18] Ware, Alan.. The American Direct Primary: Party Institutionalization and Transformation in the North. Cambridge University Press. 2002

[19] van Buuren, S., & Groothuis-Oudshoorn, K.. MICE: Multivariate imputation by chained equations in R. *Journal of Statistical Software* 45(3), 2011, pp. 1-67.

TABLE IV: Determinants of Perceived Ease of Use and Speed of Voting Procedure

	Ease of voting			Voting speed		
	Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	**-12.9**	**-19.6**	**-7.5**	**-14.5**	**-22.1**	**-6.9**
Qualification of authorities: none/little to quite a lot/very	**4.0**	**1.3**	**7.2**	**12.4**	**7.1**	**18.0**
Needed help: no to yes	**-13.1**	**-21.4**	**-6.9**	**-15.9**	**-26.3**	**-7.1**
Previous e-voter: no to yes	1.9	-0.8	4.6	**6.2**	**1.5**	**10.8**
Split ticket voter: no to yes	1.6	-1.0	4.1	0.8	-4.4	5.5
Lives in Capital: no to yes	2.7	-0.4	6.0	**13.5**	**8.1**	**19.2**
Age: 24 to 49	**-2.7**	**-5.5**	**-0.3**	3.0	-1.8	7.6
Female: no to yes	-1.0	-3.5	1.7	4.1	-0.6	9.0
Information scale (0-3): 0 to 1	-0.7	-4.3	0.9	-1.4	-6.5	1.8
Technology use scale (0-6): 3 to 6	0.4	-2.4	2.9	3.1	-1.1	7.5
Belief technology simplifies life: agree to agree a lot	**3.1**	**2.1**	**4.3**	**5.6**	**2.7**	**8.2**
Education: incomplete 2ry to complete 3ry	0.9	-1.2	3.1	-1.1	-4.9	2.6

Note: Ease of voting is coded 1 if “easy” or “very easy”, and 0 if “difficult” or “very difficult”. Voting speed is coded 1 if “fast” or “very fast”, and 0 if “slow” or “very slow”. Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

TABLE V: Determinants of Perceived Ease of Use of Different Features of the Voting System

	Ease of instructions			Ease of inserting ballot			Ease of using touchscreen			Ease of finding choice		
	Effect	95% C.I.		Effect	95% C.I.		Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	**-3.0**	**-6.9**	**-0.1**	**-18.4**	**-26.3**	**-11.3**	**-5.8**	**-10.7**	**-1.9**	**-14.0**	**-20.9**	**-8.1**
Qualification of authorities: none/little to quite a lot/very	1.9	-0.3	4.3	-2.2	-6.2	1.7	**4.2**	**1.4**	**7.1**	**7.3**	**3.7**	**11.2**
Needed help: no to yes	**-10.8**	**-18.9**	**-5.1**	**-19.6**	**-29.2**	**-11.4**	**-9.4**	**-17.0**	**-3.6**	**-10.3**	**-18.0**	**-3.5**
Previous e-voter: no to yes	1.8	-0.1	3.8	2.1	-1.8	5.8	-2.4	-5.6	0.2	1.4	-2.3	4.8
Split ticket voter: no to yes	0.1	-2.1	2.0	0.2	-3.7	4.1	-0.4	-3.4	2.1	-0.8	-4.7	2.4
Lives in Capital: no to yes	2.0	0.0	4.4	3.1	-0.4	7.9	-0.8	-3.4	1.9	-1.4	-4.8	2.2
Age: 24 to 49	-1.3	-3.4	0.5	0.6	-2.8	4.1	-0.5	-2.7	1.9	-1.0	-4.2	2.0
Female: no to yes	-0.7	-2.6	1.2	-2.5	-5.8	1.2	-0.6	-3.0	2.1	-0.4	-3.6	2.9
Information scale (0-3): 0 to 1	**0.4**	**0.1**	**0.8**	0.4	-3.0	1.7	**0.7**	**0.4**	**1.1**	1.2	-0.2	1.7
Technology use scale (0-6): 3 to 6	1.0	-0.9	2.7	0.6	-3.4	4.3	0.8	-1.7	3.2	-1.9	-5.8	1.5
Belief technology simplifies life: agree to agree a lot	**1.7**	**0.9**	**2.7**	0.7	-2.1	3.1	**3.0**	**2.0**	**4.0**	**2.4**	**0.2**	**4.3**
Education: incomplete 2ry to complete 3ry	0.1	-1.3	1.5	-2.2	-4.9	0.5	**-2.7**	**-4.6**	**-0.9**	-1.0	-3.6	1.5

Note: Responses to questions related to the ease of use of different features of the voting system are coded 1 if "easy" or "very easy", and 0 if "difficult" or "very difficult." Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

TABLE VI: Determinants of Overall Evaluation and Preference for Traditional Voting

	Evaluation system			**Preference for traditional voting**		
	Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	**-11.9**	**-19.8**	**-5.1**	**11.4**	**2.8**	**19.9**
Qualification of authorities: none/little to quite a lot/very	**14.7**	**9.9**	**20.0**	**-24.5**	**-31.7**	**-17.0**
Needed help: no to yes	**-8.4**	**-17.0**	**-1.2**	**14.7**	**3.5**	**24.5**
Previous e-voter: no to yes	-0.4	-5.4	4.0	3.6	-3.9	10.9
Split ticket voter: no to yes	-0.4	-5.2	4.1	-0.4	-7.6	7.0
Lives in Capital: no to yes	3.0	-2.0	7.5	0.2	-6.8	7.3
Age: 24 to 49	-1.9	-5.9	2.5	1.2	-4.9	7.7
Female: no to yes	0.8	-3.6	4.7	-2.1	-9.1	5.2
Information scale (0-3): 0 to 1	**-5.0**	**-11.3**	**-0.1**	4.3	-0.2	7.9
Technology use scale (0-6): 3 to 6	1.9	-2.9	6.3	**-7.8**	**-14.9**	**-0.4**
Belief technology simplifies life: agree to agree a lot	**6.6**	**4.4**	**8.5**	**-22.0**	**-27.2**	**-16.0**
Education: incomplete 2ry to complete 3ry	-2.6	-6.1	1.1	-3.3	-8.7	2.3

Note: General evaluations of the system are coded 1 if "good" or "very good", and 0 if "bad" or "very bad". Preferences for traditional voting are coded 1 if the voter reports that she/he would have preferred to vote using the traditional voting system, and 0 otherwise. Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

TABLE VII: Determinants of Perceptions of Confidence in the Integrity of the Election Process

	Confidence vote recorded			Confidence ballot secrecy			Election in Salta are Clean		
	Effect	95% C.I.		Effect	95% C.I.		Effect	95% C.I.	
Problem voting: no to yes	-6.9	-14.8	0.2	**-11.0**	**-20.0**	**-2.0**	-1.5	-9.7	7.0
Qualification of authorities: none/little to quite a lot/very	**16.6**	**10.6**	**22.6**	**23.3**	**15.7**	**29.9**	**22.1**	**14.8**	**29.6**
Needed help: no to yes	-3.0	-12.2	5.3	-1.5	-12.2	9.5	-1.3	-10.6	8.9
Previous e-voter: no to yes	-0.1	-6.1	5.7	2.9	-4.0	9.4	3.9	-2.7	10.5
Split ticket voter: no to yes	-3.0	-8.9	2.6	-3.7	-10.3	3.5	1.1	-5.5	7.7
Lives in Capital: no to yes	0.3	-5.6	6.2	**-8.9**	**-16.2**	**-1.8**	**-9.2**	**-15.9**	**-2.6**
Age: 24 to 49	-1.4	-6.8	4.3	2.9	-3.5	9.1	4.5	-1.4	10.7
Female: no to yes	2.9	-2.7	8.7	0.4	-6.0	7.1	-2.6	-9.0	3.7
Information scale (0-3): 0 to 1	-0.2	-4.6	2.9	**-5.6**	**-9.6**	**-0.6**	-1.2	-4.9	3.3
Technology use scale (0-6): 3 to 6	-0.7	-6.6	4.6	-3.6	-10.8	3.6	-4.5	-10.7	2.5
Belief technology simplifies life: agree to agree a lot	**8.0**	**4.6**	**10.9**	**12.4**	**8.0**	**17.0**	**17.7**	**11.5**	**23.8**
Education: incomplete 2ry to complete 3ry	-2.7	-6.9	1.8	0.3	-5.1	5.4	2.8	-2.3	8.1

Note: Confidence that the vote was correctly recorded is coded 1 if “sure” or “very sure”, and 0 if “unsure” or “very unsure”. Confidence in ballot secrecy us coded 1 if “confident” or “very confident”, and 0 if “not confident” or “not at all confident”. Perceptions of cleanness of elections in Salta is coded 1 if “very clean” or “somewhat clean”, and 0 if “not very clean” or “not at all clean”. Effects should be interpreted as the change in the probability that the dependent (column) variable takes value one as a result of a marginal change in the independent (row) variable. Bold figures denote statistically significant effects, at a 5% confidence level. N = 981.

E-voting in the Netherlands; past, current, future?

Leontine Loeber
University of East Anglia
Norwich, UK
Leontine_loeber@xs4all.nl

***Abstract*—This paper is a case study of a country in which e-voting used to be the general norm until 2006; the Netherlands. Since the abandonment of e-voting, several attempts have been made to reintroduces some form of e-voting. This paper describes these attempts and tries to give an insight in the possible future developments of e-voting in the Netherlands.**

Keywords— e-voting, case study.

I. INTRODUCTION

The Netherlands was an early adapter of e-voting. Voting machines were introduced in 1966 in a couple of municipalities. Since then, their use grew rapidly, so that during the municipal elections of March 2006 nearly 99% of the voters cast their vote with the use of a voting machine. Both in the 2004 European Parliament elections and the national elections of November 2006, voters abroad could vote through the internet. Since 2007 this use of e-voting dramatically declined. Nowadays, elections are conducted using paper ballots, mail ballots and hand counting. The action group ´We don't trust voting machines´ raised concerns regarding the safety of both the voting machines and the internet voting system. This ultimately led to the decision to quit using these systems and to reassess e-voting in the Netherlands. [1] However, the discussions on the use of e-voting haven't stopped.

When looking at debates concerning e-voting in public elections, two key issues have to be addressed by any e-voting solution. The secrecy of the vote has to be protected, while voters, political parties and other actors have to be able to check if votes are stored and counted as they were cast. [2] The main point that the action group raised was the impossibility to check the integrity of the Direct Recording Electronic Voting Machines (DRE) that were used (Fig.1). However, the issue of secrecy of the vote got the most attention in the debate, due to the fact that this is one of the few criteria for elections that is laid down in international law.[1] Because states have to guarantee free, fair and secret elections, in court cases that the action group started against the approval of the DRE's, they had to focus on the issue of the secrecy more than on the issue of integrity.

Fig. 1. The DRE that was used in the majority of municipalities.

II. E-VOTING IN THE POLLING STATION

After the abandonment of the DRE's that were used in the polling stations a governmental committee made recommendations on the electoral process in general and on new ways of e-voting in particular. In their report 'Voting with Confidence' [3] they recommended a new form of e-voting which would consist of a voter printer and a vote counter. A voter would make its vote on the printer, which would only print the vote. The print would then be put into a ballot box and counted at the end of the day using the vote-counter, by means of scanning it. A group of technical experts were asked if this system would be feasible and how it should be tested. Their findings were that it would be hard to ensure that this new system would meet the criteria for safety and secrecy of the vote. One particular issue that would be difficult to address was the compromising radiation that vote printers would send out, which could be used in order to breach the secrecy of the vote.[2] The Secretary of State therefore informed the Parliament that she would not pursue this system. [4]

The 2009 elections for the European Parliament were the first nation-wide elections held with the use of paper ballots and hand counting. Although the hand counting process meant that it took longer for the results to be known, most municipalities finished their counts before 3 AM election night. (Fig.2).

[1] See for example article 3 of the First Protocol of the European Convention on Human Rights.

[2] In the Dutch debates the term Tempest was used. The official term for eavesdropping by means of electromagnetic emissions is Van Eck phreaking.

Fig. 2. Example of the counting process in the Netherlands.

There were also no major incidents with voters using the paper ballots. In response to question by Parliament on the duration of the counting process, the Secretary of State emphasized that the speed with which the results are known is not a goal in itself. What is important is that the voting process, including the counting of the votes is transparent and verifiable. [5] During the municipal election of March 3rd 2010, there were 15 municipalities out of the 394 that held recounts. These recounts did not lead to changes in the seat distribution. In 2010 the Parliamentary elections were observed by the Office for Democratic Institutions and Human Rights. In their report they agree with the decision to cancel e-voting as an appropriate measure in view of the challenges to electoral integrity that were identified in 2006.

Due to complaints from municipalities about the counting process and the fact that recounts were held, the government decided in April 2010 to examine if it would be feasible to introduce a form of e-counting. A bill was drafted to make experiments with e-counting possible in 2012. However, while the Minister was investigating what requirements should be met before such an experiment could take place, Parliament once again started pushing for e-voting by means of a voting computer. The Electoral Council also showed support for the reintroduction of voting machines. [6] The Minister decided to stop focusing on e-counting in order to look at e-voting again. [7]

In 2013 the government set up a new committee to investigate if e-voting could and should be used. This committee published a report called 'Every vote counts – Electronic voting and counting', in December 2013. [8] The committee concluded that it would benefit the election process to use electronic means to count votes and preferably also to cast votes. The committee presented a model using a vote printer and vote counter. This model allows voters with a physical disability to vote without help[3] while the use of the vote counter eliminated the problems with the inaccuracy of hand counting. It is possible to check the integrity of the system because the printed votes can be hand counted to verify the tally by the vote counter. This committee therefore reached the same conclusion as the committee in 2007.

The government will look into the feasibility of the advised system of a vote printer and a vote counter. The government admits that the Tempest problem which was the reason not to introduce this system after the previous committee in 2007, still exists. However the government takes the stand that if certain measures are taken to reduce Tempest as much as possible, it is acceptable to allow for a certain level of residual risk. [9]

III. INTERNET VOTING

After the discussions surrounding the internet voting for voters living abroad during the national elections of 2006, the Minister had defined criteria that all forms of e-voting should meet. Part of these criteria are the recommendations of the Council of Europe on the use of e-voting. [10] The proposed internet voting system for the waterboard elections in 2008 failed to meet these criteria. A major issue was the robustness of the cryptography that would be used. According to the testing agency, the chosen method of encryption would in the best scenario protect the secrecy of the vote until 2030, but it would be very likely that it would be possible (way) before that date to reconstruct which voter voted for which candidate. Another issue was that a voter with the right software would be able to calculate valid voting codes within 20 hours. Since the voting period was two weeks, this would mean that such a voter would be able to cast at least 16 valid votes. Finally, there were security issues with the system that would be used. [11] The government therefore decided to withhold the certification of this system. [12] The waterboard elections were then held by the use of paper ballot mail votes.

The voters living abroad also used paper ballot mail votes during the European Parliament elections of 2009 and the parliament elections of 2010 and 2012. The main issue for these voters receiving and returning their ballot paper in time. In order to solve this issue, voters were enabled in 2012 to download and print the ballot paper themselves. This eliminates the time it takes to send the ballot papers from the Netherlands to the voter (Fig. 3 and 4).

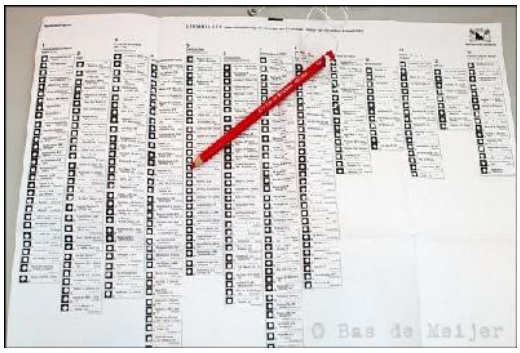


Fig. 3. Regular ballot paper.

[3] A vote printer can be equipped with audio support, making it possible for blind voters to cast their vote on their own.

Fig. 4. Ballot paper for voters living abroad.

In 2013, the Minister commissioned a market research institute to investigate the feasibility of internet voting. [13] Based on their study [14], the government informed Parliament on March 21st 2014 that they had decided that currently there are too many risks with internet voting. Combined with the large costs of internet voting and the fact that there is no evidence that internet voting raises turnout, the government will not introduce internet voting for voters living abroad in the near future. [15]

IV. Debates in Parliament

Before the Parliamentary elections in 2006 during which the controversy on e-voting arose, the Dutch Parliament was a big supporter of e-voting. Most parties were in favor of introducing nation-wide internet voting. In the first two years after the 2006 elections, the view on e-voting was dramatically different. Parliament supported the decision to cancel e-voting as long as the issues concerning secrecy and integrity were not solved. In 2007 it was Parliament who questioned the possible use of internet voting for voters living abroad. Most members felt that the internet voting system might not meet the criteria for secrecy of the vote and integrity and asked for criteria such a system should meet. [16] The decision in 2008 to cancel the use of internet voting for the waterboard elections was also supported by Parliament. In these debates, both issues; secrecy and integrity, were mentioned by members as reasons not to use e-voting. However, this attitude towards e-voting changed after the first elections conducted with paper ballots. Both after the European Parliament elections of 2009 and after the municipal elections of 2010, members asked the Secretary of State to investigate the return to e-voting, because hand counting was both inaccurate and time-consuming. [17] Where members stressed the importance of the integrity of the vote in February 2012, [18] in December 2013, nearly all political parties in Parliament were in favor of using e-voting, because that hand counting was inaccurate. [19]

V. 'Stemfies'

A question that recently got attention in the Dutch voting process is the use of smartphones by voters to make a 'stemfie' (a picture of themselves voting). During the municipal elections of March 2014, a politician posted a photo of himself on social media on which his face and the marked ballot paper were visible, showing his vote (Fig.5). His example was followed by many voters. In answer to questions about these photos, the Minister said that these kind of photos are not prohibited under Dutch law. A ngo then started a procedure against the Minister in which they demanded that he would issue a statement that 'stemfies' are not allowed and that the polling stations should act against them, because 'stemfies' breach the secrecy of the vote. On May 9th 2014, the judge ruled that although the disadvantages of 'stemfies' were in his eyes bigger than the advantages, the Election law does not prohibit them and therefore there was no reason for the Minister to withdraw his statements. During the European Parliament elections, a sign in the polling stations informed voters that they didn't have to reveal their vote to anyone.

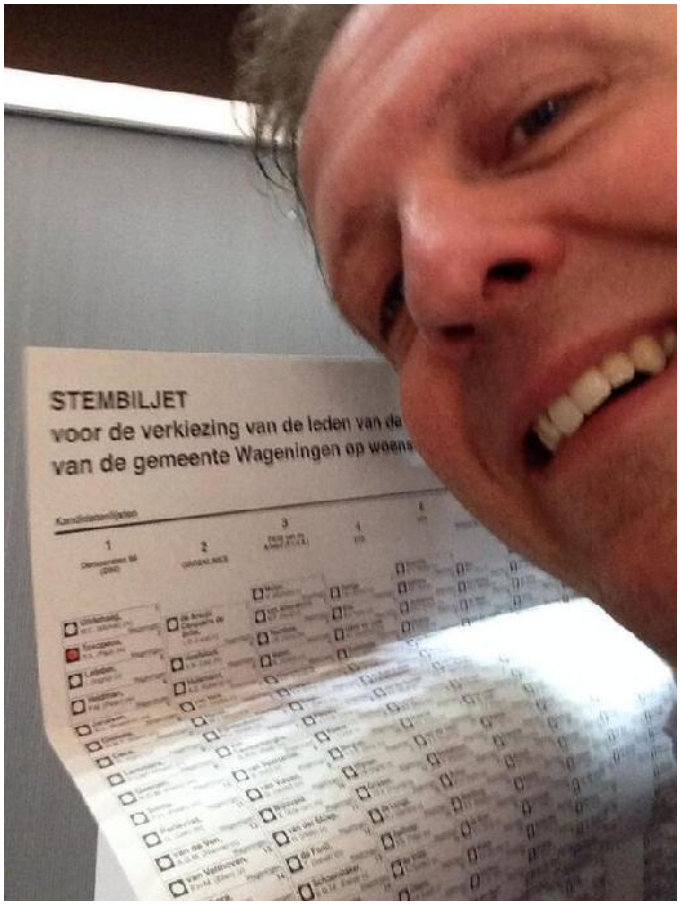


Fig. 5. 'Stemfie'.

VI. Conclusions

Although the events of 2006 led to a withdrawal of all forms of e-voting in the Netherlands and caused debates in Parliament, shortly after, Parliament once again asked for the introduction of new forms of e-voting. Both committees that looked into e-voting recommended the same: a vote printer combined with a vote counter. While government did not follow this advice in 2007 due to the concerns on secrecy of the vote and integrity of the system, nowadays it seems willing to embrace this system. Further research will be done to discover if such a system is feasible, and possible to implement in a cost-efficient manner. The government however has made the decision not to pursue internet voting for voters living abroad.

What is striking about the debate in the Netherlands on e-voting is the short time that elapsed between the decision to abandon e-voting and the renewed call for it from election officials and members of Parliament. Where the main focus was on the protection of the secrecy of the vote and the integrity of the system, it shifted to the (perceived) inaccuracy of hand counting. The arguments against e-voting seemed to have faded into the background in favor of the arguments against voting by paper ballot. One argument that is used in the debate is that paper ballot voting is old-fashioned and that in the Netherlands, where computers are a big part of daily life, it should be possible to use technology in the voting process. It is questionable if this argument should play a role in a debate that should focus on questions of secrecy of the vote, integrity of the system and accuracy of the results.

Besides the issues of e-voting and internet voting, the use of smartphones by voters to make ‘stemfies’ and post them on social media gives rise to a new debate on secrecy of the vote. Is this a right that a person can waive, or is it also a duty of a voter to protect the secrecy of the vote? At this moment, this question remains unresolved, but will undoubtedly play a role in future debates on the Dutch election process.

References

[1] L. Loeber, “E-voting in the Netherlands; from general acceptance to general doubt in two years.” Electronic voting 2008, GI lecture notes in informatics, ed. R. Krimmer and R. Grimm, 21-30. Bonn, Germany: Gesellschaft für Informatik.

[2] L. Mitrou, D. Gritzalis and S. Katsikas. "Revisiting legal and regulatory requirements for secure e-voting." Security in the Information Society. Springer US, 2002. 469-480.

[3] F. Korthals Altes et. al., “Voting with confidence”, Report by the Election Process Advisory Commission September 27, 2007, found on www.minbzk.nl.

[4] Kamerstukken II 2007/08, 31 200 VII, nr. 64.

[5] Kamerstukken II 2009/10, 31 142, nr. 16.

[6] Evaluation report of Septermber 22nd 2010, found on www.kiesraad.nl.

[7] Kamerstukken II 2013/14, 31 142, nr. 37.

[8] Committee reseach electronic voting in the polling station, “Every vote counts, Electronic voting and counting”, Kamerstukken II 2013//14 33 829, nr. 1.

[9] Kamerstukken II 2013/14, 33 829, nr. 3.

[10] Legal, operational and technical standards for e-voting, Rec(2004) 11.

[11] Fox-it, “Rapportage advisering toelaatbaarheid internetstemvoorziening waterschappen”, August 12th 2008.

[12] Kamerstukken II 2007/08, 31 142, nr. 11.

[13] Kamerstukken II 2013/14, 31 142, nr. 39.

[14] Kamerstukken II 2013/14, 33 829, nr. 2.

[15] Kamerstukken II 2013/14, 33 829, nr. 3.

[16] Handelingen II November 21st 2007, 26-2017 – 26-2023.

[17] Handelingen II 2009/10, Aanhangsel 267 and Kamerstukken II 2009/10, 31 142, nr. 22.

[18] Kamerstukken II 2011/12, 31 142, nr. 33.

[19] Kamerstukken II 2013/14, 31 142, nr. 39.

Implementation Project
Electronic Voting Azuay 2014 – Ecuador

Juan Pablo Pozo Bahamonde
National Electoral Minister
National Electoral Council (CNE)
Quito, Ecuador
juanpozo@cne.gob.ec

I. BACKGROUND

After the general elections held on February 17, 2013 , the National Electoral Council became committed to improve the electoral process through the introduction up-to-date voting and counting technologies .

A number of responsible and serious studies were carried out ever since in order to assess the feasibility of implementing the Electronic Voting by multidisciplinary teams. Given the current legislation in Ecuador and especially, the cultural reality found in Azuay province, a third-generation software solution was chosen, the same that incorporates a single ballot with an embedded chip and an electronic voting machine, all in one single system .

Generalities regarding the implementation electronic voting in the province of Azuay, local elections 2014

The project executory unit was embodied by the Provincial Delegation of Azuay. The overall objective was to implement a pilot electronic voting process in the voting and counting stages for the election of sectional authorities to be held in February 2014 in the province of Azuay.

The following specific objectives were set in order to attain this objective:

- To build knowledge base on the electronic voting in order to perform automated elections in the nation.
- To establish the regulatory framework for electronic voting and its implementation.
- To implement automatic processing in voting machines, producing results in a timely and reliable manner.
- To carry-out audits at all stages of the electronic voting.

The pilot plan was implemented in an entire province in order to measure and assess the impact of electronic voting within the voting, counting and totalization stages and to evaluate the overall results with regard to the authorities who are elected in a specific region (Prefect, vice-prefect, municipal mayors, urban and rural municipal councilors, and members of rural parish councils), It was decided to conduct the pilot project in the province of Azuay, based upon the following considerations:

- Azuay has 2.163 voting boards which is 5, 5% of the nation's total.
- The number of voters per each voting station has been kept in (300). One equipment shall be placed in each voting station (2163 equipments in total).
- Twenty per cent of the equipments were assigned to training exercises (440 equipments) whereas 10% were assigned for contingencies (220 equipments).
- The Electoral Province Delegation is skilled in the implementation of electronic voting processes.
- The mentioned Province Delegation has a high level of efficiency in the implementation of electoral processes.
- Staff in Azuay province is adequately trained for the implementation of this kind of projects.
- Adequate means of transportation (road and air) make it easy to transport the voting equipments and allow a good communication between the work teams and the CNE headquarters.
- There are good roads from Cuenca city to all the voting sites throughout the province.

TABLE I. POPULATION DATA

Population data
Azuay province presents the greatest percentage of young population: 46.7% between 15 and 44 years of age.
53.2% of the province young population are women
It is the third most densely inhabited province.

Fig. 1. Geographical location of Azuay province

Azuay is a province located south of Ecuador in the Southern Sierra Region (Andes). Its northern border meets the province of Canar, on the south the provinces of El Oro and Loja, on the east the provinces of Morona Santiago and Zamora Chinchipe, and the province of Guayas to the west. Its capital city is Cuenca, a city known as the "Athens of Ecuador" with some 330,000 inhabitants in the urban area.

II. Analysis to Determine the Best Tool

In order to decide which technology should be used to automate the voting and/or counting process, technological, legal and procedural aspects were taken into account, including the political culture in our country (both in terms of political parties and movements, and citizens in general). Within this framework (once the technology to be implemented was selected), it was possible to start making all necessary contacts throughout Latin American countries for their support with the techology solution that had been chosen. This, because variables such as language, technical support, transportation, among other aspects made it easier to locate the electronic voting method that was applied in our country.

Legal, procedural and technical aspects were taken into account in order to ensure the following conditions: *Universal Suffrage, Equal Suffrage, Free Suffrage, Suffrage Secrecy, Transparency, Verification, Reliability and Safety.* Additionally, all voting options were considered, including null and blank ballots.

As for the integral procedural standards, Calling for elections, Voters, Candidates, Voting process, Results, and Audit were taken into consideration. Also, the following technical standards were considered: Accessibility, Interoperability, Operating Systems, Security, Audit and Certification. Necessary recovery procedures were taken in case of a system failure so that the data would not be lost. The electronic voting system had restricted access levels according to the specific tasks performed by the different users.

Measures were adopted to ensure adequate system protection against intrusions from outside. Transmission of results was safeguarded through the utilization of safe transmission means that guaranteed data integrity and accuracy. The proposal was aimed at improving the quality of electoral processes in charge of the CNE by delivering accurate and verifiable results in the shortest possible time. The final objective is to improve the exercise of political rights of citizens through the implementation of automatic mechanisms within the voting and counting processes.

As per the above (as shown in the chart below), the electronic voting machine with smart ballot proved to be the most adequate for application within the Ecuadorian electoral system. Thus, it was suggested to the CNE Board that the technology that best fits the electoral process and that could deal with the number of candidates for the electoral process of February 23th, 2014, was the electronic voting equipment with smart paper ballot. However, the main problem with electronic voting is that it does not stick to Article 10 of the Organic Law of Elections and Political Organizations of the Republic of Ecuador which provides that popular voting must be publicly scrutinized.

TABLE II. COMPARISON OF VOTING TECHNOLOGY

Feature	*Electronic Ballot Box*	*Styluz*	*Smart Ballot*
Audit of voting at voting station	X	X	X
Voting secrecy	X	X	X
Counting celerity	X	X	X
Equipment portability		X	X
Electrical autonomy			X
Celerity and safety in the transmission of results gathered at each voting station	X		X
Displays candidate information on screen / ballot	X		X
Votes counted in public			X
MJRV-enabled suffrage process.	X	X	X
Accessibility for people with dissabilities.	X		X
Low propability of ballot loss (with votes /voting receipts)		X	X
Vote modifications are not possible during the counting process.	X		X
TOTAL *	8	6	12

III. COMPETITIVE ADVANTAGES OF ELECTRONIC VOTING COMPARED TO MANUAL VOTING

- Experiences in the region are favorable (in some provinces of the Republic of Argentina, this system has been used successfully in voting processeses. More than 900,000 voters from different social and cultural levels use it).
- Vote counting is public and can be observed and validated by different observers and representatives of political sectors.
- It allows to set-up the software according to the election type: It accepts blank and null ballots, votes per lists of candidates and different languages, including Quichua and Spanish. Interface designers made sure that all possibilities are available on the screen.
- 100% auditable throughout all process stages.
- The device where the vote is cast does not store any information; the choices are stored in an RFID chip on the ballot and are printed on it.
- It facilitates voting of people with disabilities including a module for the blind. One of the advantages is that the electronic equipment can be used in various voting processes, which implies an economic benefit.
- Fully portable equipment.
- It does not link the voting station with the equipment, voters can choose any free machine for your vote.
- The voter may request another ballot in case of noticing a mistake.

IV. IMPLEMENTATION OF THE ELECTRONIC VOTING PROJECT

The e-voting project was developed precisely in response to the need of obtaining agile, verifiable and transparent voting results, taking into account today's global demand for free and widespread citizen access to information, knowledge and networking, through the use of digital tools to reduce the technological gap. Moreover, the implementation of electronic voting generates a substantial change in all aspects, with politics and governance as two areas of great importance, leading to a rethinking on the proper relationship between candidates and voters as well as between representatives and citizens.

The proposal on which we based this proposal was a thorough improvement in the quality of electoral processes in charge of CNE and the generation of accurate and verifiable election results in the shortest possible time. The purpose is to improve the application of citizens' political rights by introducing automated mechanisms within voting and counting processes.

V. LEGAL FRAMEWORK

According to the constitutional mandate, the National Electoral Council shall ensure the exercise of people's political rights through their votes as provided for by the Organic Electoral and Political Organizations Law of the Republic of Ecuador, Code of Democracy, enforcing

principles of effectiveness, efficiency and quality that the public administration must observe.

Moreover, by implementing the electronic voting (which does not require the use of ballots), we will provide all aids and adequate safety levels in accordance with article 109 of the Code of Democracy. For instance, we will attain the participation of all voters and will provide the aid required by people with disabilities so that all of them will be able to vote.

The National Electoral Council may also decide to use electronic methods not only during the voting but also for the counting stage, for which purpose all rules can be modified if necessary (based upon Articles 113 and 115 of the Code of Democracy).

VI. Electronic Voting. An effective solution to a ballot counting process

Ecuador has been manually managing the processes of voting and counting of votes at polling stations and the recount in the Provincial Election Boards, with consequent problems that may arise in the manipulation of electoral kits and ballots, problems such as: ballot size, number of candidates to be elected, interpretation of some votes cast, errors in transcribing the data from vote registers, slowness in delivering results and the possibility of human errors in the counting of votes. Consequently to the above mentioned, the CNE decided that it was necessary to introduce automatic voting and counting processes. The implementation of a new computer voting system and the use of modern vote counting tools conveyed risks within the implementation and operation stages. Therefore, such implementation was programmed by stages with specialized area teams dully trained to take over project implementation.

The management team was formed with officials from the head office specialized in areas related to information, communication, finance, logistics, legal, administrative, training and electoral processes.

VII. Project's communicational dimension

A population study was carried-out in Azuay province as part of a communicational strategy. It was found that over 60% of Azuay inhabitants did not have a clear idea regarding the Electronic Voting, reason why we started an aggressive informative and training program. The campaign included visits to local communication media to spread communication products such as written newsletters, informative reports including audio interviews on the main activities undertaken by the election authorities and a monthly press conference on the progress of the project.

A massive campaign was launched in order to reach a large segment of the population. The campaign included radio, television, and print media with highly informative and emotive contents to inform people from Azuay regarding the electronic voting process. Once people were aware of the ELECTRONIC VOTING and its advantages, they rushed to the nearest training point in order to learn more about the new technology to be applied. They were also receptive to receive the training conducted at their workplaces.

The communication ELECTRONIC VOTE campaign was present on the main social networks used by people from Azuay, networks that spread positive messages on the project (always highlighting the benefits of using technology in favour of our democracy). The communications department received important feed back through this means, including many opinions issued by citizens. Additionally, the ELECTRONIC VOTE project included mobile training at a bus equipped with electronic voting machines that traveled all around the 15 cantons of the province of Azuay.

VIII. Strategies employed to promote the training process

It began with a socialization through two seminars on electoral processes that took place in the city of Cuenca with the participation of experts in the topic, experts such as Carlos María Ljubetic (Paraguay), Rui Santos (Portugal) and Amilcar Brunazo (Brazil). The workshops were aimed at the population in general and were attended by media, university representatives, representatives of the neighborhoods of Cuenca, provincial authorities and political organizations. These experts were able to share personal experiences in each of their countries.

Management of electronic voting developed the training plan that was launched in the province of Azuay. It is worth mentioning the training given to MJRV's (members of polling stations and actors involved in the event) on the management and operation of the Electronic Voting machine used in the electoral process of 23 February 2014.

Undoubtedly, we were aware on the importance of providing adequate training to voters (general public) on the voting machine.

Training started on October 1, 2013 with the first group of 100 trainers who received information about the e-voting process, voting machines, laws and hints on how to approach to people. Training to citizens started on October 15th with the 22 computers available at that time. Until 16th November 2013 a total of 100 equipments were available for the training events to citizens, including social, professional, corporate, institutional and the public in general.

In total we counted with the participation of some 200 trainers who toured throughout the province providing training at public and private companies, schools (to parents of students), universities, students from upper high school years, neighborhoods, rural communities, political organizations and at the most crowded places such as markets, parks, bus terminals, fairs and churches.

TABLE III. TRAINING

Inhabitants	Voters	% of registered voters	Number of trained citizens	Percentage of trainees
609.007	459.303	75,42%	367.441	80 %

Source: Delegation of Azuay province.

IX. SYNERGY BETWEEN TECHNOLOGY AND ELECTORAL MANAGEMENT

The Electronic Voting Project provided tools that facilitated interaction with the voting process, tools such as is the voting introduced in Azuay province on 11 December 2013, a tool that was available to citizens and political organizations at www.cne.gob.ec and www.cnezona4.ec. This tool allowed practices from home.

Functioning of the "QR Code" was explained to political organizations for them to keep quick records on the results obtained at polling stations in the province of Azuay, including details on the operation of the software's source code to allow political organizations to carry-out their own ballot counting.

Network

200 transmission links were installed with a bandwidth of 1Mbps, featuring transmission of coded information. Transmission in nationwide links reached 150 Mbps with optic fiber, which guaranteed a fast delivery of information to the ballot counting hub. XDSL technology was used in copper-based networks at rural areas. Wireless links (Radio) were established in areas lacking wire networks, as well as mobile suppliers working on 3G APN technologies. VSAT-satellite technology links were installed in areas with difficult geographical access.

X. AUDITING PROCESS: A WARRANTY OF TRANSPARENCY AND RELIABILITY

Four electronic voting audits were conducted in Azuay project. There, voters and political organizations were able to verify the results of the election process.

Audit of installation, voting and counting software - In this audit software installation, voting and counting were validated through observation, review of the application and generation of a hash code that ensures the integrity of the software used in voting and counting processes.

Audit database - This audit was performed to review the databases used as a repository of the information generated at every voting site and was used o generate the final results.

Audit of the scrutiny made at the Poll Station - This audit was conducted by the Electoral Provincial Board of Azuay and consisted of performing manual counting every vote for prefect and Vice-Prefect , Mayors, Urban - Rural Councillors and Members of the Rural Parish Boards. Once the votes counted , were compared with the results of the electronic totalizing system .

Audit of the totalization system - This audit was conducted by the Electoral Provincial Board and involved the processing of ballots for Prefect, Vice-Prefect, Mayors, Rural Councillors and Members of the Rural Parish Boards. The results were totalized and compared with the results of the electronic totalization.

XI. MUTUALITY BETWEEN THE ELECTRONIC VOTING PROJECT AND THE INCLUSION PROJECTS CENTERED AROUND HISTORICALLY EXCLUDED GROUPS.

As for the "Voting at Home" project, the National Electoral Council (CNE) developed a plan that allowed people with disabilities and older adults to vote at home by leveraging the portability of the electronic voting equipment. A database of persons with disabilities requiring special attention was elaborated before the elections. Prisoners at state jails in Azuay province were also able to vote thanks to the electronic voting machines with intelligent ballot.

XII. VARIABLES OF A COMPREHENSIVE ASSESSMENT

The following was obtained on 23 February 2014 at the Sectional Elections 2014:

1) Result reporting in less than two hours upon voting closure;
2) Reduction of absenteeism from 31.38% in 2009 to 24.80% in 2014;
3) Training given to more than 525,000 people (standing for 78% of voters).
4) Audit of 100% of voting registers and technical audits on pre-election, election and post-election phases.
5) 39 people suffering from disabilities voted at home.
6) 241 jail prisoners were given the right to vote (those who had not been sentenced).
7) Inter-cultural voting of indigenous people (in their native language).
8) Signing of the "Agreement for our Democracy and Transparency" supporting the electronic voting process (signed by political organizations participating in the electoral event).
9) Positive acknowledgements from observing missions that deem e-voting as an emblematic electoral project.

10) Permanent support given by people who became empowered of the E-voting project held in Azuay 2014.

XIII. Comparative Analysis of Participation from 2009 to 2014 (sample: province Prefect, Mayor)

The elections held on February 2014 showed an increasing participation of citizens. Comparing with the elections held in 2009, absenteeism fell from 31.38% to 25.21% in 2013 at province level, ending at 24.54% in the last elections held in February 2014. If you want to compare the amount of blank and null votes that were obtained from one election to another, it is necessary to compare two similar elections, 2009 being the last electoral process in which sectional authorities were elected. It is noteworthy that the electronic voting itself eliminates unintentional errors made by voters. It also eliminates the subjective interpretation of votes by polling station officials. Considering the results obtained in 2009 for province Prefect we can see that the number of blank votes in 2014 was smaller. A different behavior occurs in null ballots... there were fewer nulled ballots in 2014 than in 2009. (See comparison chart).

TABLE IV. Nulled Ballots 2009 – 2014 Prefect

	Election April 2009 – Prefect	Election february 2014 – Prefect
Population	551.291	609.007
Voters	378.423	459.303
Polling stations	2.319	2.163
Blank	44.041	34.716
Nulle	28.553	30.662
Total Blank and Nulle votes	72.594	65.378
Absenteeism	31.38%	24,58%

Regarding blank and null ballots for mayors, an increase in the number of blank votes was seen in 2014 compared to 2009 and a decrease of null votes from 2009 to 2014. The increase of blank and null votes from 2009 to 2014 is just 10.35 % despite the number of voters grew in that period by 16.69 %.

The total percentage of blank and null votes for Mayor with regard to the number of voters is 16.45% in 2009, whereas in 2014 such percentage dropped to 15.31 %. Participation level has also grown in Cuenca canton during the last election, going from 70.60 % in 2009 to 76.48 % this year.

TABLE V. Nulled Ballots 2009 – 2014 Mayor

‘	Election April 2009 – Mayor	Election february 2014 – Mayor
Voting sites	1.573	1.464
Voters	383.253	424.847
Persons who voted	270.682	324.918
Blank	16.044	27.016
Null	28.553	22.731
Total Blank and Nulle votes	44.597	49.747
Absenteeism	29.40%	23.52%

ANNEX. PERCEPTION OF VOTERS TOWARDS THE IMPLEMENTATION OF THE ELECTRONIC VOTING PROJECT IN AZUAY PROVINCE.

Methodology - The questionnaire was aimed at those voters who had just cast their electronic vote: A questionnaire was designed for the survey. The surveys were conducted at voting stations with the sample selected.

The questionnaire consisted of multiple choices (related to voters' socio-economic condition, variables concerning their confidence toward electronic voting, new voting technologies and scope of information campaigns and training conducted by the e-voting project weeks before the Election Day). Additionally, the questionnaire allowed respondent voters to recommend or suggest solutions to the problems derived from citizen's eagerness to know and improve the system for the next elections.

Sample design - The sample design was stratified, randomized and configured by county and urban area. Rural areas and voting sites according to the number of voters in the province of Azuay.

RESULTS FOR AZUAY PROVINCE

A total of 3,983 individuals were surveyed in Azuay province (distributed in 36 polling stations in urban and rural areas).

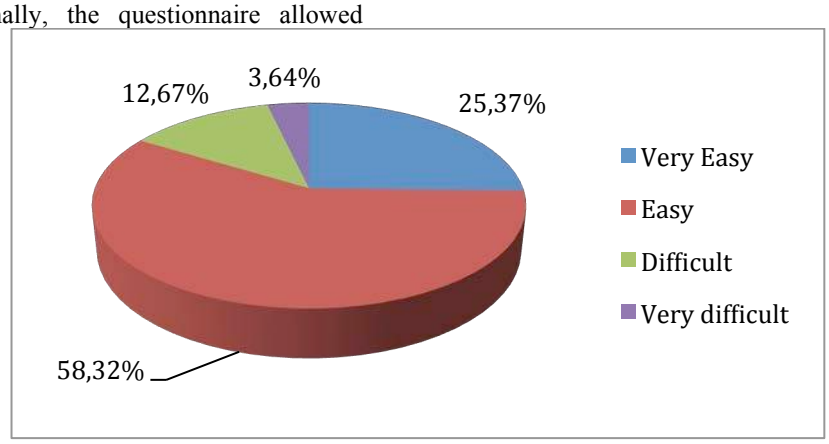


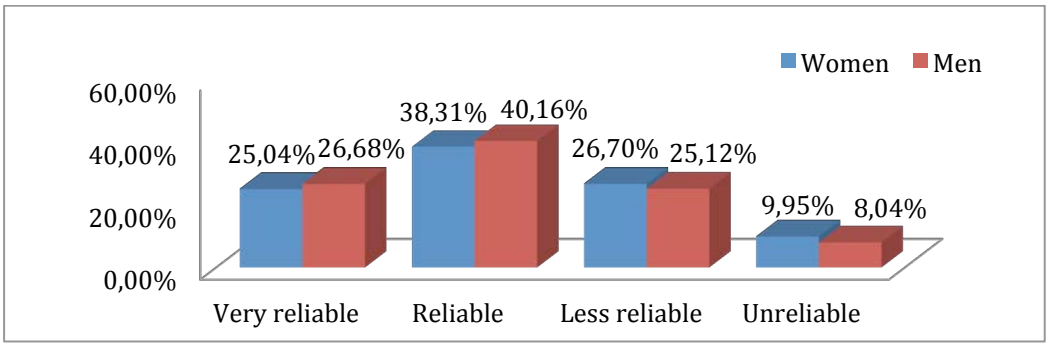
Fig. 2. Rating of Experience of Electronic Voting

1. *How do you qualify the experience of electronic voting in Azuay?*

This first rating evidence that the majority of voters surveyed (more than 80 %) felt that their experience to vote electronically was very easy or easy, which indicates a certain way that the electronic voting project Azuay was successful. Certainly, it is necessary to check that the components that formed each of the projects require adjustments, so that we can improve these processes in future projects. Below are the voters' perceptions of women and men separately.

TABLE VI. RATING OF THE EXPERIENCE OF ELECTRONIC VOTE BY SEX

AZUAY PROVINCE		
	Women	Men
Very reliable	25.04%	26.68%
Reliable	38.31%	40.16%
Less reliable	26.70%	25.12%
Unreliable	9.95%	8.04%



In conclusion it can be inferred that the fact of being a man or a woman does not affect the rating of the experience of the electronic vote; that is to say, the electronic vote was qualified in equal proportions by both voters and women voters by men.

Another key aspect of the research revolves around the voter confidence in front of the electronic voting system in Azuay. It is important to note that it is one thing that the voter has been found with a voting system friendly and easy to use; while another thing is that the voter qualifies as reliable or not the voting system as such. Hence the importance of understanding on the part of the voter, if despite having found an electronic voting system easy to use or not, the voter found reliable or not the voting system.

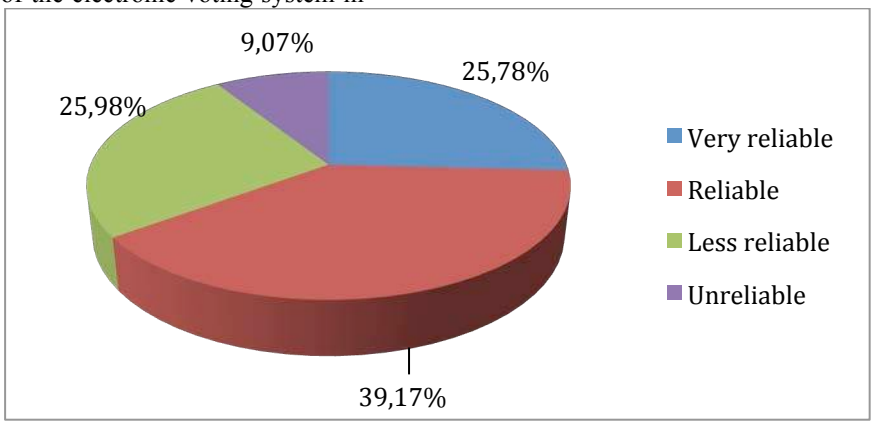
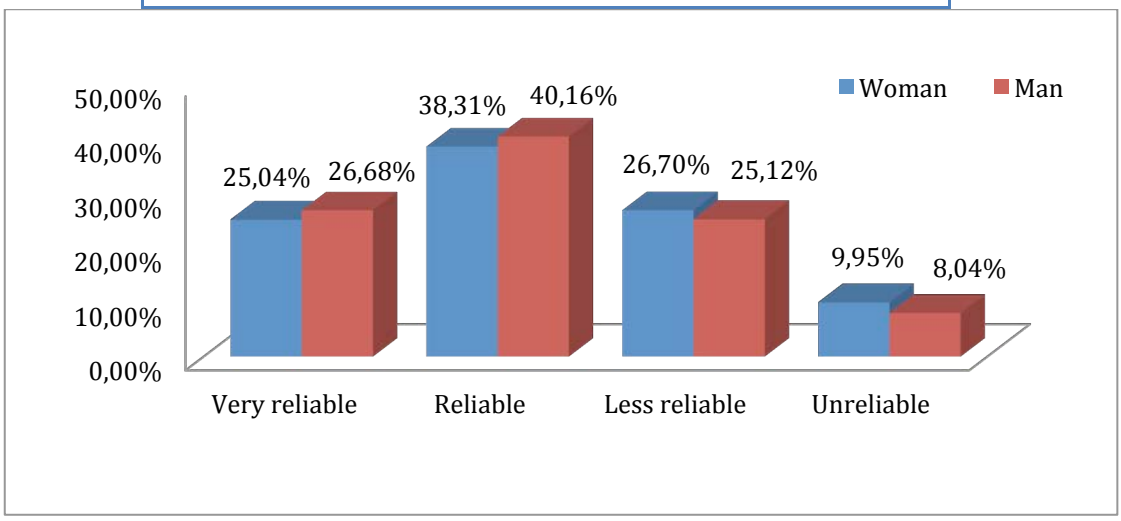


Fig. 3. Reliability in e-voting

At this point, the research i wanted to know the perception of voter with regard to this topic. The results reveal perceptions divided among voters who considered the system very reliable (25.78 %), reliable (no 39.17 %), unreliable (25.98 %) and nothing reliable (9.07 %).

TABLE VII. RELIABILITY IN E-VOTING

AZUAY PROVINCE		
	Women	Men
Very reliable	25.04%	26.68%
Reliable	38.31%	40.16%
Less reliable	26.70%	25.12%
Unreliable	9.95%	8.04%



2. *Are you willing to use this system for the upcoming elections?*

For the National Electoral Council is essential to know the opinion of citizens on whether voters would be willing to use the electronic voting system that were used in their respective provinces for the coming elections or not. Below are the results of this question along with the sex variable.

In general, eight out of ten people would be willing to vote using the electronic voting system that used the day of the election in their respective provinces. Similar results when viewed from the sex variable are presented below.

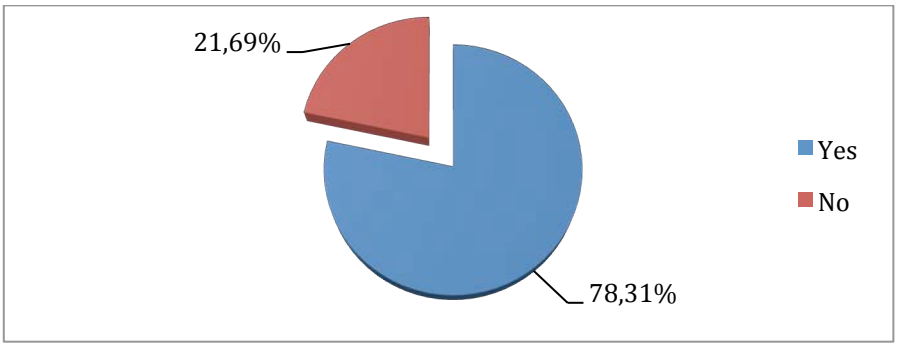
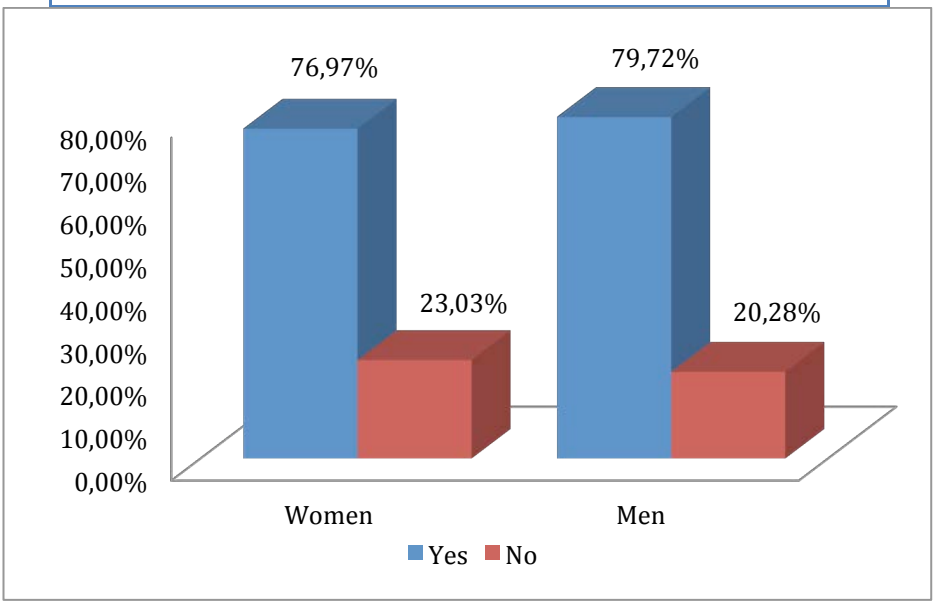


Fig. 4. Use or electronic voting in future electoral processes of the Azuay Province Reliability in electronic voting

TABLE VIII. USE OF ELECTRONIC VOTING IN THE UPCOMING ELECTIONS BY SEX

AZUAY PROVINCE		
	Women	**Men**
Yes	76.97%	79.72%
No	23.03%	20.28%

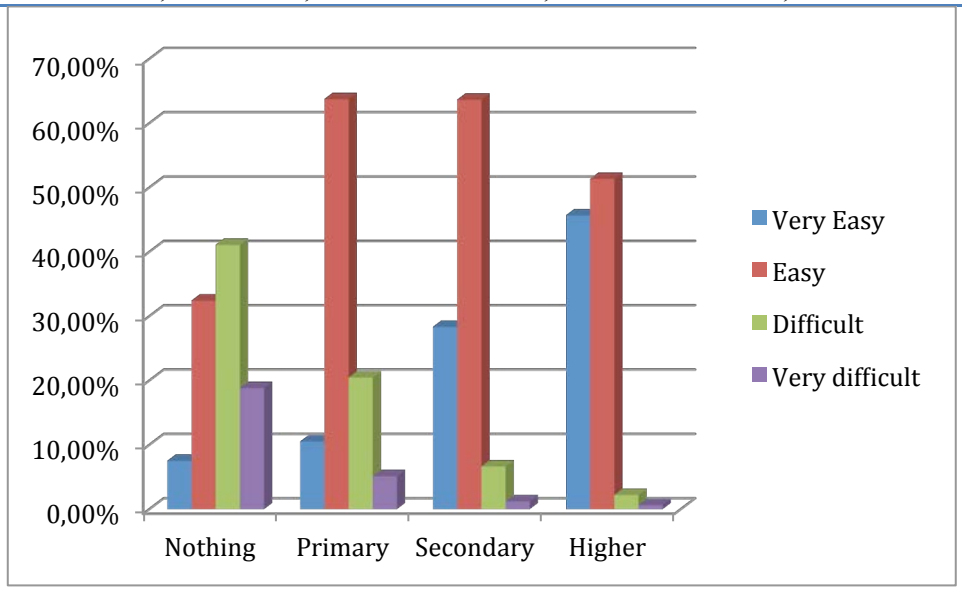


3. *Experience of electronic voting by level of education?*

In the following graphic shows how the voters felt the ease or not on the use of the voting machine depending on their level of education. In this way there is for example that a higher level of education, the easier it is considered the use of the machine.

TABLE IX. EXPERIENCE OF ELECTRONIC VOTING BY LEVEL OF EDUCATION

AZUAY PROVINCE				
	Nothing	Primary	Secondary	Highger
Very easy	7,55%	10,55%	28,38%	45,70%
Easy	32,45%	63,78%	63,69%	51,37%
Difficult	41,13%	20,50%	6,69%	2,25%
Very difficult	18,87%	5,16%	1,24%	0,68%

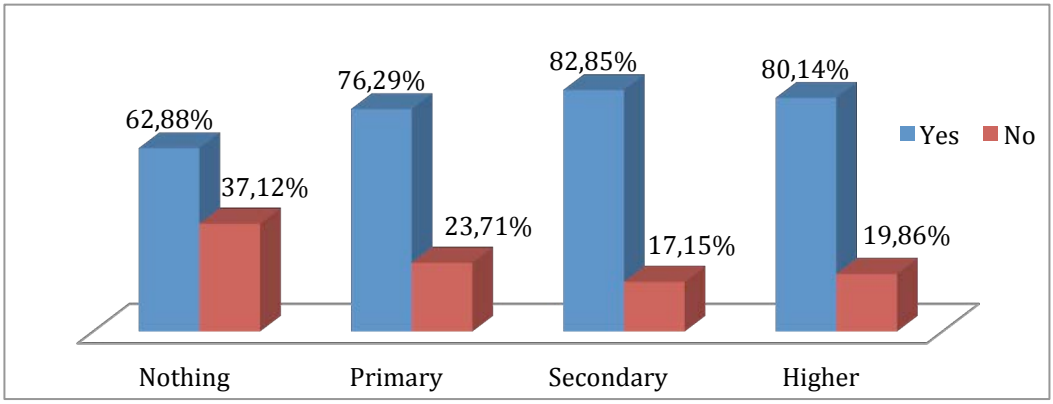


4. Confidence in the electronic voting systems by level of education?

The following graphs shows that the digital divide in terms of confidence is tied to the level of education of the electorate: the higher the level of education, the greater the confidence to the system. For the province of Azuay, the 80.14 % of people with higher education rely on the system:

TABLE X. CONFIDENCE TO THE SYSTEM ACCORDING TO LEVEL OF EDUCATION

AZUAY PROVINCE				
	Nothing	Primary	Secondary	Higher
Yes	62,88%	76,29%	82,85%	80,14%
No	37,12%	23,71%	17,15%	19,86%

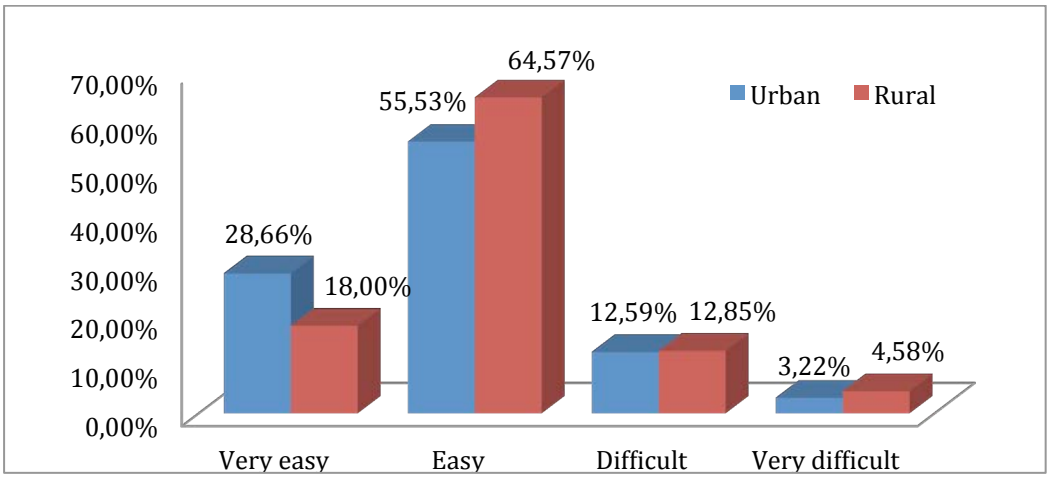


5. *Urban and rural behavior with regard to electronic voting in Azuay?*

It is important to know how the electorate of the urban and rural areas felt with regard to electronic voting. Below are results, considering primarily the variable ease of use of the machine and confidence to the system.

TABLE XI. RATING OF THE EXPERIENCE OF ELECTRONIC VOTING IN URBAN AND RURAL AREAS AZUAY

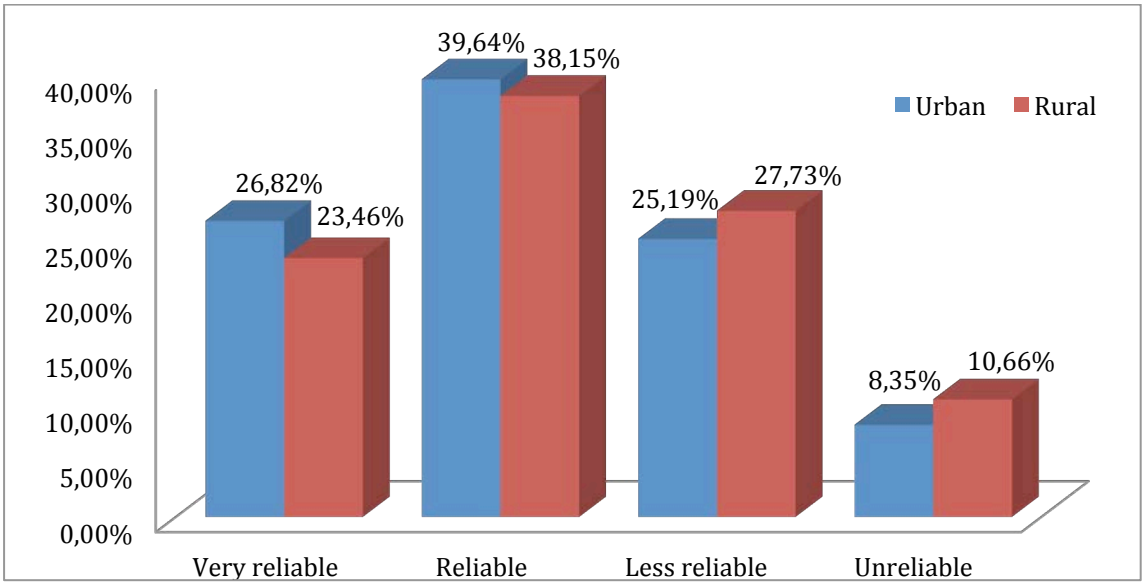
AZUAY PROVINCE				
	Very easy	Easy	Difficult	Very difficult
Urban	28,66%	55,53%	12,59%	3,22%
Rural	18,00%	64,57%	12,85%	4,58%



It can be seen that there is no significant relationship between urban or rural area and the qualification of the voter to the use of electronic voting machine. In other words, for both urban voters as to the rural was observed similar results. Below are the results based on the variable trust to the voting system.

TABLE XII. CONFIDENCE AS URBAN OR RURAL AREA

AZUAY PROVINCE				
	Very reliable	Reliable	Less Reliable	Unreliable
Urban	26,82%	39,64%	25,19%	8,35%
Rural	23,46%	38,15%	27,73%	10,66%



It should be noted that for both the variable ease of use of the machine as to the variable trust the electronic voting system, urban areas have a considerable increase on the rural areas with regard to the ease of use and the confidence to the system. On the other hand, rural areas manifested in greater numbers than urban areas, that the use of the machine is not easy and that the voting system is not reliable. These answers may have its origin in the level of education of the voters polled.

Practicality of Technical Solutions

Efficient End to End Verifiable Electronic Voting Employing Split Value Representations

Michael O. Rabin
Harvard SEAS
Columbia SEAS
Email: morabin@gmail.com

Ronald L. Rivest
MIT CSAIL
Cambridge, MA 02139
Email: rivest@mit.edu

***Abstract*—We present a simple and fast method for conducting end to end voting and allowing public verification of correctness of the announced vote tallying results. In the present note voter privacy protection is achieved by use of a simple form of distributing the tallying of votes and creation of a verifiable proof of correctness amongst several servers, combined with random representations of integers as sums mod M of two values. At the end of vote tallying process, random permutations of the cast votes are publicly posted in the clear, without identification of voters or ballot ids. Thus vote counting and assurance of correct form of cast votes are directly available. Also, a proof of the claim that the revealed votes are a permutation of the concealed cast votes is publicly posted and verifiable by any interested party. We present two versions of the method, one assuring voter privacy and proof of correctness in the presence of information leaking devices, the other achieving the same goals as well as prevention of denial of service by failing or sabotaged devices.**

Advantages of this method are: Easy understandability by non-cryptographers, implementers, and ease of use by voters and election officials. Direct handling of complicated ballot forms. Independence from any specialized cryptographic primitives. Verifiable mix nets without using public-key or homomorphic cryptography, a novel result of significance beyond e-voting. Speed of vote-tallying and correctness proving: elections involving a million voters can be tallied and proof of correctness of results posted within a few minutes.

I. Introduction and Overview

End-to-End Verifiable Voting (E2EVV) systems provide high confidence that errors and fraud can be detected and that the announced election outcome is correct. See [1]–[5] for some surveys and results about E2EVV. Cramer et al. [6] have also used secret-sharing to ensure robustness of a voting system, as we do in Section X. Recently, E2EVV systems have been used in actual elections [2] and are proposed for use in new systems such as the STAR-Vote system in in Travis County (Austin) Texas [7].

The parties and agents involved in our E2EVV scenario are:

Voters: We assume n voters V_1, V_2, ..., V_n.

Tablets: Each voter uses a tablet to compose her vote. The tablet can also print out a receipt for the voter.

Election authorities: Individuals responsible for running the election.

Election Servers: Computers performing specific functions in the election.

Secure Bulletin Board (SBB): An election server providing a secure public append-only record of election-specific data, including all cast ballots, the final election outcome, and a proof of correctness of the election outcome.

Proof Server: An election server that produces a proof of correctness of the election outcome. In our method, the proof server is implemented with a two-dimensional array of independently-controlled computers; these servers are also servers in our mix-net implementation (so we also call them "mix-servers").

Tally Server: An election server that computes the election outcome from the publicly posted list of decrypted cast votes.

Adversary: The adversary attempts to cause an incorrect election outcome to be accepted. (An accepted proof of correctness as presented here, assures correctness of announced tally outcome no matter how the adversary acted.) An adversary may also attempt to violate the privacy of voters.

An election then comprises the following steps:

1) **Setup:** The list of eligible voters is determined. The list of ballot questions is determined. (For presentation purposes we assume only one question on the ballot, which may nonetheless require a complex answer such as a preference ordering of the choices. For more questions the entire method may be repeated.) Cryptographic keys are set up as necessary for tablets and election servers.
2) **Vote Casting:** Each voter uses a tablet to enter her choice on the ballot question. The system uses some convention for providing each ballot with a unique ballot id bid. The choice is "encrypted" (more on that later), and sent to the election servers with the bid. The voter is given a printed receipt with the bid and the hash of the encryption.
3) **Posting of Vote Records:** The bid's and encrypted choices are posted on the SBB at the end of election day.
4) **Verification of Postings:** Voters may access the SBB to verify that the encryptions of their choices are correctly posted (comparing their receipt with the hash of the posted encryption for their ballot).
5) **Mixing:** The mix servers anonymize the encrypted ballots by permuting their order and dissociating the encrypted ballots from identifying meta-data such as voter names or bid's. Each of $2m$ copies of the list

of n encrypted ballots is independently mixed and re-encrypted. The resulting $2m$ permuted lists are posted on the SBB.

6) **Random Challenge:** A "random challenge" (a long string of random digits) is derived by hashing the SBB contents and/or from a public dice-rolling ceremony. The unpredictability of this challenge to an adversary prevents the adversary from undetectably manipulating the election outcome.
7) **Proving consistency with cast votes:** A random half (determined by the random challenge) of the $2m$ lists of encrypted ballots are partially decrypted, to check that the mixing was properly done. The method used here depends on properties of split-value vote representations to ensure that voter privacy is preserved. The partial decryptions are posted on the SBB for all to confirm.
8) **Posting and verification of election outcome:** The other half of the $2m$ lists are all fully decrypted and posted on the SBB. Anyone may check that they are identical lists (albeit differently permuted). The final election outcome may be determined from any one of these lists.

Adversarial model. We assume that the adversary is trying to "rig" an election by trying to force an incorrect election outcome to be accepted (because it appears to have been proven correct) or to learn how some particular voters have voted.

In Sections III–IX the adversary is assumed *not* to be interested in causing the election to fail (that is, to not produce an election outcome or proof of correctness at all). Section X deals with adversaries who attempt to deny service by failing.

Innovations re other E2E methods. The elements of our end-to-end voting method are reasonably standard, except that

- Ballots are "encrypted" in a novel manner, using commitments to secret-shared split-value representations of the voters' choices.
- No modular exponentiations or public-key operations are required, yielding substantial efficiency improvements.
- The mix-net operation is proved correct in a new manner: rather than proving each step of the mix-net to be correct, the overall operation is proved correct.
- Because ballots are fully decrypted for the final tallying operation, there is no restriction on the tallying method used. Complex tallying rules (e.g. IRV) and write-in candidates are easily handled. Furthermore, no zero-knowledge proofs are required that the encrypted ballots are valid.

We thus show how using Rabin's Split Value Representation (SVR) of integers method greatly simplifies an E2E implementation. SVR methods have been proposed for implementation of secure auctions [8], [9]; the extension to voting involves, however, further innovations.

The current paper extends our previous works [10], [11] exploring such innovations; In particular, we note that our earlier work [10] has the problem that a single election server must know how everyone voted; the present work remedies that defect.

Outline of paper. We begin in Section II with some preliminary notation and a discussion of the properties of split-value representations, including methods for securely proving equality of the values represented.

Then Sections III–IX discuss each phase of our method in detail, from initial setup to creating and verifying the final proof of correctness of the election outcome.

Section X shows how to extend the basic method to one that tolerates a certain number of failures of the mix-net servers, by using Shamir's secret-sharing method.

Finally, Section XI provides some discussion of the practical aspects of our methods, and Section XII concludes.

II. Preliminaries

A. Notation

We let $x \parallel y$ denote the concatenation of x and y.

B. Representations modulo M

For a given race, votes and values used in the system are described by values modulo a given integer M. Here M is chosen large enough so that any voter choice (including a "write-in" choice) may be represented by a unique integer modulo M. In the following, additions and subtractions of values are performed mod M.

Our methods are independent of the way such values are used to represent candidates or complex choices (as with preferential balloting).

Some of our methods (see Section X) require that M be prime.

C. Split-Value Representations

Our methods are adapted from those of [8], [9].

Definition 1: Let x be a value modulo M, so that $0 \le x < M$. A *split value representation* of x is any vector

$$X = (u, v)$$

where u and v are values modulo M such that $x = u + v \pmod M$.

Definition 2: We define the *value* of a split-value representation $X = (u, v)$ modulo M to be

$$\textsc{Val}(X) = (u + v) \bmod M \ .$$

Note that there are M different split-value representations of any given value x, since u can be arbitrarily chosen from $\{0, 1, \ldots, M-1\}$, and then the corresponding v derived via $v = (x - u) \bmod M$.

Definition 3: A *random split-value representation* of a value x modulo M is a randomly chosen split-value representation of x modulo M.

D. Commitments

Commitment to values mod M We use a commitment function $\text{COM}(K, u)$ employing a (randomly chosen) key K to commit to value u modulo M.

It is assumed that COM is computationally hiding: given the value $C = \text{COM}(K, u)$, it is infeasible to gain any information about u.

Opening a commitment $\text{COM}(K, u)$ means to reveal K and u; this opening can be verified by re-computing $\text{COM}(K, u)$.

It also assumed that it is computationally infeasible to find two pairs (K, u) and (K', u') such that $\text{COM}(K, u) = \text{COM}(K', u')$. This renders the commitment by COM to be computationally binding; no one can open a commitment in more than one way.

COM can be implemented, say, by use of AES with 256 bit keys, or with the HMAC cryptographic hash function.

We sometimes write $\text{COM}(u)$ instead of $\text{COM}(K, u)$, with the understanding that a randomly chosen K is used (which is revealed with u when the commitment is opened).

Commitment to split-value representations

Our use of a commitment to a split-value representation is analogous to the "encryption" of a choice in other E2E methods.

Definition 4: A *commitment* $\text{COMSV}(X)$ *to a split-value representation* $X = (u, v)$ is a pair of commitments, one to each component:

$$\text{COMSV}(X) = (\text{COM}(u), \text{COM}(v)) \ .$$

Note that $\text{COMSV}(X)$ denotes commitment to a split-value vector representation of a value x, $0 \leq x < M$, while $\text{COM}(u)$ is a commitment to a value u, $0 \leq u < M$.

The following fact is crucial to the security of our methods.
Fact. If just one of the two coordinates u or v in a commitment to a random split value representation X of a value x is opened, then no information about the value x is revealed.

E. Proving equality of commitments

The nice thing about commitments to split-value representations is that they can be (probabilistically) proved equal without revealing the values represented.

Suppose a Prover asserts that

$$\begin{aligned} \text{COMSV}(X) &= (\text{COM}(u_1), \text{COM}(v_1)) \\ \text{COMSV}(Y) &= (\text{COM}(u_2), \text{COM}(v_2)) \end{aligned}$$

represent the same value: $\text{VAL}(X) = \text{VAL}(Y)$. To prove this, the Prover first reveals t, where

$$t = u_2 - u_1 \pmod{M} \text{ and} \quad (1)$$
$$t = v_1 - v_2 \pmod{M} \quad (2)$$

The Verifier then picks a random value $c \in \{1, 2\}$; if $c = 1$ he asks the Prover to open $\text{COM}(u_1)$ and $\text{COM}(u_2)$. Otherwise, the Prover must open $\text{COM}(v_1)$ and $\text{COM}(v_2)$. The Verifier correspondingly checks (1) or (2). The Prover fails if the checked equation fails.

Fact. If $\text{VAL}(X) \neq \text{VAL}(Y)$, then the Prover fails with probability at least 1/2.

It is very important that a given split-value commitment should not participate in more than one such proof. Otherwise both its components may be revealed, thus revealing the value represented.

Generalization to tuples We use a generalization of the above proof method, wherein X is replaced by a tuple X_1, X_2, X_3 such that $\text{VAL}(X) = \text{VAL}(X_1) + \text{VAL}(X_2) + \text{VAL}(X_3)$, and similarly for Y and Y_1, Y_2, Y_3. (This is for our default three-row proof server arrangement; more values are used if there are more rows.)

A proof of the equality that

$$\text{VAL}(X_1) + \text{VAL}(X_2) + \text{VAL}(X_3) = \\ \text{VAL}(Y_1) + \text{VAL}(Y_2) + \text{VAL}(Y_3)$$

proceeds just as before, except that opening the first component of X is replaced by opening the first component of each of X_1, X_2, and X_3, and opening the second component of X is replaced by opening the second component of X_1, X_2, and X_3; similarly for Y. Again a value t such that $X_1 + X_2 + X_3 = Y_1 + Y_2 + Y_3 + (-t, t)$ is posted by the Prover.

The basic fact (that a cheating Prover is unmasked with probability at least 1/2) remains true.

F. Proving Equality of Arrays of Vote Values

We further generalize such proofs of equality to proofs of equality for lists of length n of commitments to vote values.

In our mechanism votes are represented by triplets $T = (X, Y, Z)$ and committed to as

$$\text{COMT}(T) = (\text{COMSV}(X), \text{COMSV}(Y), \text{COMSV}(Z)) \ .$$

By definition,

$$\text{VAL}(T) = (\text{VAL}(X) + \text{VAL}(Y) + \text{VAL}(Z)) \bmod M \ .$$

Assume that a Prover has posted in a SBB two arrays of commitments to triplet representations of values:

$$\text{COMT}(T_1), \text{COMT}(T_2), ..., \text{COMT}(T_n)$$
$$\text{COMT}(T'_1), \text{COMT}(T'_2), ..., \text{COMT}(T'_n).$$

The Prover claims that $\text{VAL}(T_j) = \text{VAL}(T'_j)$ for $1 \leq j \leq n$.

To post a proof of correctness on the SBB, the Prover posts the values $t_1, \ldots, t_n$ required for proving the claimed equalities.

Afterwards, employing appropriate randomness (see Section VIII), n random independent values $c_j \in \{1, 2\}$, $1 \leq j \leq n$, are computed and posted by the Verifier.

Now the Prover constructs and posts a corresponding proof for each claimed equality $\text{VAL}(T_j) = \text{VAL}(T'_j)$, $1 \leq j \leq n$, which can be verified as shown above.

Theorem 1: If more than k of the claimed n value equalities are false then the probability of acceptance of the claim is at most $(1/2)^k$.

Proof: If for an index j, $\text{VAL}(T_j) \neq \text{VAL}(T'_j)$, then the probability of the inequality not being uncovered is at most $1/2$. Because of the independent random choice of the challenges $c_j \in \{1,2\}$, $1 \leq j \leq n$, the probability of not uncovering at least one of the k inequalities is most $(1/2)^k$. ■

This completes our review of the mathematical preliminaries needed for our methods.

III. SETUP

We now begin our more detailed description of our method, beginning in this Section with the Setup phase.

See Figure 1 for a graphic depiction of the overall method.

A. Choice of M

We assume that there is only one race in the election. (The entire method can be replicated for additional races.)

A value of M is chosen so that each possible choice a voter can make in this race (including write-in votes, if allowed), may be uniquely represented as a value w, where $0 \leq w < M$.

If the extensions of Section X are used that use Shamir's secret-sharing method [12] to handle failing servers, then M should be prime.

B. Tablets and Servers

The voter casts her vote in a voting booth by use of a Tablet. Multiple voters may vote on a single Tablet. A representation of the vote is transferred as described below from the Tablet to various to election servers.

Some of the servers are "mix servers" that anonymize the vote by removing identifying information and shuffling them according to a secret permutation.

The mix servers also act collectively as a "proof server" (PS) that prepares a publicly verifiable proof of the correctness of the election results.

The proof of correctness will be publicly posted by the PS on an electronic Secure Bulletin Board (SBB) accessible to voters, parties involved in the election, and the general public.

In this note, to achieve high assurance of voter privacy the PS consists of nine independent devices $P_{1,j}$, $P_{2,j}$, $P_{3,j}$, $j = 1, 2, 3$ (considered as three rows of three devices each).

It will be demonstrated that as long as no more than two devices may leak out information, privacy of voters is protected. Generalizations for other parameterizations will be described later. The obvious generalization to the case of ℓ leaky devices employs $(\ell + 1)^2$ devices.

C. Secure Channels

We assume that suitable arrangements are made for secure channels between the tablets and the election servers.

For example, one may use three pairs (e_j, d_j) of a public-key encryption method (PKE), for $j = 1, 2, 3$. Here e_j is a public encryption key, and d_j is the corresponding secret decryption key. Every voter Tablet has all public encryption keys e_j, $j = 1, 2, 3$. Every $P_{j,1}$ has the secret decryption key d_j .

However, in such an implementation, the public-key decryption may become an overall computational bottleneck. Thus, we recommend using a simple hybrid encryption method to set up private symmetric keys, employing only one PKE encryption key per tablet and the corresponding PKE decryption key by the Proof Server per Tablet. This reduces the overall PKE decryption time significantly.

Each proof server also has secure channels to every other proof server in the same row or column.

IV. VOTE CASTING

We assume that the Voter's Tablet is given (or creates) a unique ballot id bid for each voter.

The Voter's Tablet takes the Voter's V vote w, where $0 \leq w < M$, and randomly represents w as a triple (x, y, z) such that

$$w = (x + y + z) \bmod M \ .$$

It then creates random split-value representations of x, y, and z as $X = (u_1, v_1)$, $Y = (u_2, v_2)$, and $Z = (u_3, v_3)$. Tablet chooses for X random keys K_1, K_2 and sends to $P_{1,1}$ the ballot representation:

$$bid, \text{COMSV}(X), PKE(e_1, (K_1, u_1) \parallel (K_2, v_1)))$$

where

$$\text{COMSV}(X) = (\text{COM}(K_1, u_1), \text{COM}(K_2, v_1)).$$

Similarly a message containing $\text{COMSV}(Y)$ is sent to $P_{2,1}$ and a message containing $\text{COMSV}(Z)$ is sent to $P_{3,1}$, using different pairs of random keys for each commitment, and using e_2 for encryption for $P_{2,1}$, and e_3 for encryption for $P_{3,1}$. In this way the Tablet sends to the first device in each row a portion of a distributed representation of vote w (each portion being a commitment to a split-value representation of a component of w, where the components add up modulo M to w).

The use of the above split value representations X, Y, Z, for x, y, z, is one of the main innovations of this paper. It is used in creating the publicly verifiable proof of correctness of the submitted votes and of the tally of the election.

As part vote-casting, the voter may participate in a "*cast-or-challenge*" protocol see Benaloh [13] to verify that her Tablet has faithfully represented her choice(s). We omit details.

V. POSTING OF VOTE RECORDS

In E2EVV each ballot is encrypted and posted on a secure public append-only Bulletin Board (SBB) [14].

All encrypted ballot information received from Tablets is publicly posted on the public Secure Bulletin Board, so that voters may confirm their correct reception. To simplify procedures, a voter is given on her receipt the ballot id bid of her vote, and the postings may be in order of ballot id.

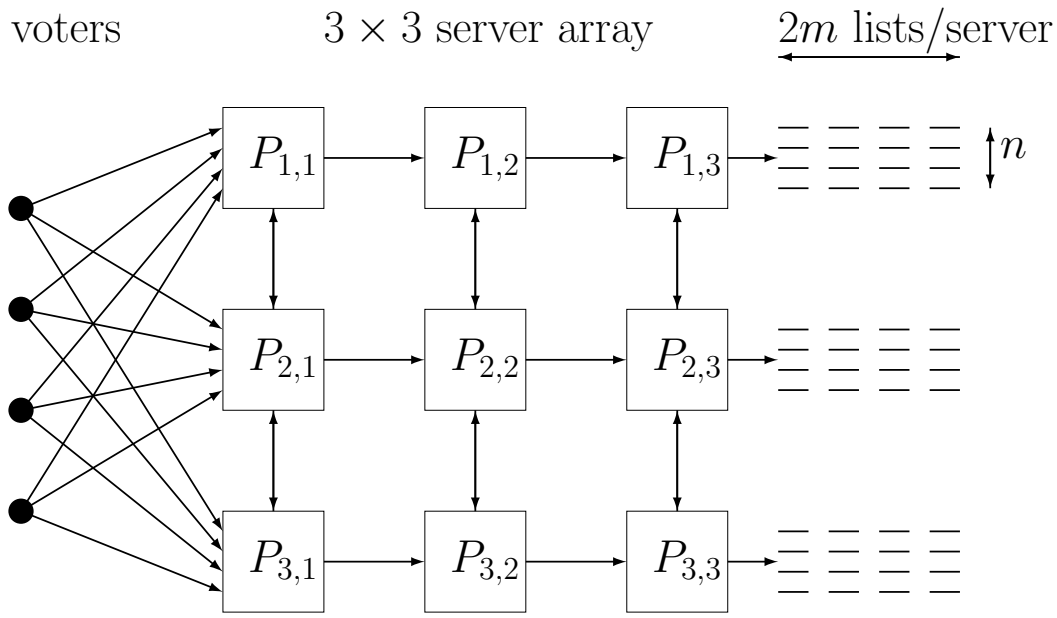


Fig. 1. An illustration of the method for $n = 4$ voters. Information flows from left to right. Each voter sends an encrypted share of his vote to each of the servers in the first column; these encrypted shares are also posted on a secure bulletin board. Each column obfuscates and reshuffles its data (each server in a column using the same random permutation) before sending it on to the next column. The information flow from the first column to the output is repeated $2m = 4$ times (with different randomness used each time). A "cut-and-choose" method randomly selects m columns of output lists to be re-routed back to be compared for consistency with the input. The other m columns are opened, checked for consistency, and posted to reveal the election outcome. A proof of the correctness of the election outcome is then prepared and posted, as described in the text.

VI. Verification of Postings

The voter was given a paper receipt from the Tablet giving a hash value of what should be posted, to enable simple verification of correct inclusion of her ballot.

Every voter can then verify that the cipher text of her ballot has been properly posted, this without her being able to convince anybody what her actual vote was. (The voter does not know how to open any commitments.)

VII. Mixing

The implementation of a fast verifiable mix-net, described in this Section, is one of the main contributions of this paper.

We emphasize that the required computational primitives are just additions mod M of integers of value at most M, and concealment of integers u of size at most M as $\textsc{Com}(K, u)$ by a fast commitment function $\textsc{Com}(\cdot, \cdot)$. These primitives are done on individual proof servers $P_{i,j}$, not in a multi-party fashion, and are executable on ordinary laptop or desktop computers at the rate of millions of operations per second.

Our mix-net, consisting of $P_{1,j}$, $P_{2,j}$, $P_{3,j}$, $j = 1, 2, 3$, creates and publicly posts $2m$ arrays of length n, each of which is a secret random permutation of the (encrypted) votes $w_1, \ldots, w_n$.

Why are $2m$ permuted lists produced, instead of a single one, as is usual for mix-nets? The answer is that we need half of them to check against the posted inputs, and half to produce the desired election outcome. Because no split-value commitment can be compared for equality more than once, we need multiple copies to make this approach work out.

The actual number $2m$ used depends on the degree of correctness assurance the system is designed to achieve; Theorem 3 in Section IX shows that $2m = 24$ provides high assurance.

Decryption. To begin, $P_{1,1}$, $P_{2,1}$, $P_{3,1}$, each using its private decryption key, opens its received commitments.

The Proof Server PS device $P_{1,1}$ has the secret decryption key d_1. It decrypts for each Ballot component X the $PKE(e_j, (K_1, u_1) \parallel (K_2, v_1))$ part. The revealed values (K_1, u_1), (K_2, v_1) are checked as the correct opening of $\textsc{ComSV}(X)$, enabling $P_{1,1}$ computes $\textsc{Val}(X) = x = (u_1 + v_1) \bmod M$.

Now $P_{1,1}$ has the sequence of X-components $x_1, \ldots, x_n$ of the n vote values $w_1, w_2, \ldots, w_n$.

Similarly $P_{2,1}$ computes $y_1, \ldots, y_n$ and $P_{3,1}$ computes $z_1, \ldots, z_n$. Here the first vote is $w_1 = (x_1 + y_1 + z_1) \bmod M$.

Even though first-column devices now have components in the clear, the distribution of a vote value w as the sum mod M of x, y and z and sending each component to a different $P_{j,1}$, $j = 1, 2, 3$, ensures that if at most two devices are leaky, the vote remains secret.

First column obfuscates and shuffles. To create an output array consisting of the n vote values concealed and randomly permuted, the servers $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ comprising the first column of the PS first *obfuscate* and then *shuffle* the list of n vote values, before passing them on to the next column.

Obfuscating: The first-column proof servers create an *obfuscation* of the list of n vote values.

Definition 5: We say that $S'_1 = (x'_1, y'_1, z'_1)$ is an *obfuscated form* of $S_1 = (x_1, y_1, z_1)$ if

$$x'_1 + y'_1 + z'_1 = x_1 + y_1 + z_1 \pmod M ,$$

that is, if S'_1 and S_1 represent the same value.

The method for $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ to obfuscate the first vote value (represented as a triple $S_1 = (x_1, y_1, z_1)$ in the three servers) is to chose three random values p_1, q_1, r_1 in the range 0 to $M - 1$, subject to $(p_1 + q_1 + r_1) \bmod M = 0$ and to compute $x'_1 = (p_1 + x_1) \bmod M$ by $P_{1,1}$, etc. Similar obfuscation is done on the components of the other $n-1$ votes w_2 , ..., w_n using different randomly chosen triplets p_j, q_j, r_j for each obfuscation.

Shuffling: $P_{1,1}$ has now the values x'_1 , ..., x'_n, $P_{2,1}$ has the values y'_1, ..., y'_n and similarly for $P_{3,1}$. Now $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ together choose a random permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Send data to next column. Then $P_{1,1}$ transmits the array $x'_{\pi(1)}, \ldots, x'_{\pi(n)}$, to $P_{1,2}$. Similarly $P_{2,1}$ transmits the array $y'_{\pi(1)}, \ldots, y'_{\pi(n)}$, to $P_{2,2}$ and $P_{3,1}$ transmits the array $z'_{\pi(1)}, \ldots, z'_{\pi(n)}$, to $P_{3,2}$.

Second column obfuscates and shuffles. The second column $P_{1,2}$, $P_{2,2}$, $P_{3,2}$, repeats the same process of obfuscation and shuffling, sending the obfuscated-shuffled array to the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$.

Last column obfuscates and shuffles. Finally, $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ again obfuscate and shuffle so that $P_{1,3}$ has the array $(x'''_{\sigma(1)}, \ldots, x'''_{\sigma(n)})$. Similarly for $P_{2,3}$ and the array $(y'''_{\sigma(1)}, \ldots, y'''_{\sigma(n)})$ and for $P_{3,3}$. Here σ denotes the permutation of the original order of the ballots into the present arrays.

Posted of lists of votes. Server $P_{1,3}$ creates and posts on the SBB commitments $(\text{COMSV}(X'''_{\sigma(1)}), \ldots, \text{COMSV}(X'''_{\sigma(n)}))$ to split-value representations of the components $(x'''_{\sigma(1)}, \ldots, x'''_{\sigma(n)})$. Similarly, $P_{2,3}$ creates and posts $(\text{COMSV}(Y'''_{\sigma(1)}), \ldots, \text{COMSV}(Y'''_{\sigma(n)}))$ and so does $P_{3,3}$.

This total posted array of $3n$ commitments is one of the $2m$ lists produced by the mix-net; the whole process is repeated $2m$ times to obtain the set of all $2m$ lists.

Remark. Note that in our method of shuffling, unlike in mix-nets, components of votes are not shuffled amongst rows going from one column to the next. They rather stay within the same row obfuscated and in shuffled order.

Theorem 2: **(Maintenance of Voter Privacy.)** As long as no more than two of the nine servers $P_{i,j}$ leak out unintended data, there are at least one row and one column in the 3×3 array of servers $P_{i,j}$ that do not contain an improper server. This, combined with the obfuscation and shuffling from one column of servers to the next and the final obfuscation and shuffling by the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ of servers, results in complete secrecy of votes by individual voters, even if the above output arrays of $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ are made public and two servers of the PS leak out all their data.

We shall prove this theorem following the next remark. It is assumed that the communications between any two mix servers is secure.

Remark. If computations were properly done, then $(x'''_{\sigma(1)} + y'''_{\sigma(1)} + z'''_{\sigma(1)}) \bmod M = w_{\sigma(1)}$, etc. That is, from the output arrays of $P_{1,3}$, $P_{2,3}$, $P_{3,3}$, the votes $w_1, \ldots, w_n$ can be directly read off (in the order σ).

Proof: In first phase of obfuscation and shuffling going from the first column $P_{1,1}$, $P_{2,1}$, $P_{3,1}$ to the second column $P_{1,2}$, $P_{2,2}$, $P_{3,2}$, obfuscating a typical $S_1 = (x_1, y_1, z_1)$ into $S'_1 = (x'_1, y'_1, z'_1)$ by use of p_1, q_1, r_1. Note that $P_{1,1}$ keeps x_1 and x'_1 in its own memory. Similarly for $P_{2,1}$, $P_{3,1}$ and their components of S_1 and S'_1.

This implies that even though p_1, q_1, r_1 are known to all three of $P_{1,1}$, $P_{2,1}$, $P_{3,1}$, nothing is revealed about components of votes stored in non-leaky devices.

The same holds about obfuscation and shuffling going from the second column $P_{1,2}$, $P_{2,2}$, $P_{3,2}$ to the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$.

Once the third column $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ is reached either it or one of the two preceding columns do not contain any leaky device. Thus third-column outputs protect voter privacy. ■

VIII. RANDOM CHALLENGE

We note that the proof servers have a need for random values of two distinct flavors:

- *Internal randomness.* The PS needs random values to create random split-value representations random permutations, etc. These values should be unpredictable to outsiders, but need not be unpredictable to the proof servers themselves. For these purposes, the proof servers may use what we call "internal randomness": truly random sources available only to each proof server.
- *External randomness (for challenges).* The proofs of correctness need random challenges (e.g. for the cut-and-choose of m lists out of $2m$, or for the proofs of equality of split-value commitments) that are unpredictable even to the proof servers (as they may be malicious). These random challenges may be obtained in either of two ways: in the Fiat-Shamir style [15] as the hash of the current SBB, or from a random external source (e.g. a dice-rolling ceremony). The former approach has the advantage that the (pseudo-)random values obtained by hashing the SBB

may be verified by anyone, but has the disadvantage that an evil proof server may try many values to be posted on the SBB until the SBB hash is to its liking. Thus, the value of $2m$ may need to be significantly larger if the Fiat-Shamir method is used. Our analyses assume that the challenges are derived from a truly random external source; appropriate adjustments to the value of $2m$ should be applied if the Fiat-Shamir method is used.

IX. Proof of Correctness

The election outcome and associated tally, as well as a proof of correctness of the announced results, are also posted on the SBB, and can be verified by anyone.

Posting of split-value representations of mix-net outputs. The device $P_{1,3}$ creates random split-value vector representations $X'''_{\sigma(i)}$ for $x_{\sigma(i)}$, $1 \leq i \leq n$, and commitments $\text{ComSV}(X'''_{\sigma(i)})$ for $1 \leq i \leq n$. Similarly for $P_{2,3}$ with the $y'''_{\sigma(i)}$, and $P_{3,3}$ with the $z'''_{\sigma(i)}$.

Using the notation of Section II-F $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ together prepare and publicly post for $1 \leq i \leq n$:

$$\text{ComT}(T_{\sigma(i)}) = (\text{ComSV}(X'''_{\sigma(i)}), \text{ComSV}(Y'''_{\sigma(i)}), \text{ComSV}(Z'''_{\sigma(i)})) \quad (3)$$

This process of obfuscation, shuffling and posting an array of the form (3) is repeated by the PS $2m$ times, where $2m$ is chosen to yield the desired assurance of correctness. Each of these posted arrays is of course created by use of a different permutation of $\{1, \ldots, n\}$.

Cut and Choose. By use of randomness extracted from all posted data together with an independent random seed, m of the posted lists (3) are randomly chosen for a proof of value-consistency with the posted concealed votes (see Introduction).

Proving consistency with cast votes: Each of these m chosen arrays (3) is rearranged by the Proof Server in the order of of bids, hence in the order of the submitted-posted concealed ballots. This is done by backtracking for the chosen arrays, the permutations used by each column.

The permutations σ for the m chosen arrays are posted, as are the values $(t_i, -t_i)$ used in the proof. For brevity we omit the simple details of how $P_{1,3}$, $P_{2,3}$, $P_{3,3}$ compute and post the pairs $(t_i, -t_i)$, $1 \leq i \leq n$.

Now the randomness is used to open one coordinate in each of the commitments in the posted concealed ballots and the corresponding commitment in each of the m rearranged arrays (3) and prove equality of values by the method of Section II-F.

By Theorem 1, if even one of these m lists differs from the ballot list by more than k values then the probability of acceptance is at most $(1/2)^k$.

Posting and verification of the election outcome: Now all the other m permuted lists are opened and the values are revealed. Only if all opened lists are permutations of the same values is the proof of correctness accepted. The election outcome is then the result of applying the appropriate tallying function or election outcome determination function to any of the opened lists. (We assume that the election outcome does not depend on the order of the ballots.)

Level of assurance provided. We now analyze the level of assurance provided by the posted proof.

Definition 6: Call a permuted array of n values *k-good* if when re-arranged in the order of the originally concealed n ballots posted by the tablets on the PS, it differs from the concealed ballot values in fewer than k locations.

Theorem 3: The probability that the opened arrays (3) are permutations of the same values but they are not k-good, i.e. the probability of accepting an announced tally result differing from the correct tally by more than k vote values is at most

$$1/C(2m, m) + (1/2)^k \approx \sqrt{3.14m}/2^{2m} + (1/2)^k,$$

where $C(2m, m)$ is the binomial coefficient "2m choose m".

Proof: Call H the set of m lists of n ballots revealed by $P_{1,3}$, $P_{2,3}$, $P_{3,3}$. Assume that one, and therefore all, of these ballot lists is not k-good. The probability that in the cut and choose the set H is chosen to be opened is $1/C(2m, m)$. If H is not chosen then the proof of value consistency is conducted on at least one array of n concealed ballots which is not k-good. The probability of this happening and proof of correctness being accepted is at most $(1 - 1/C(2m, m))(1/2)^k$. ■

For the case of no more than 20 wrong votes we use $2m = 24$ and the probability of accepting a proof of correctness while there are more than 20 discrepancies is less than $1.38/2^{20}$.

X. Countering Denial of Service Attacks (Device Failure)

It is relatively straightforward, using well-known secret-sharing methods, to provide increased robustness against the possibility that one or more of the proof server devices may fail. As noted in the introduction, Cramer et al. [6] have also used secret sharing to improve robustness of a voting system. (Their paper employs homomorphic encryption and unlike the present work reveals only the final value of the vote count.)

These methods allow construction of systems satisfying specified robustness requirements in addition to voter privacy protection. When failures may occur, then obfuscation is done by the method of proactive secret sharing (see [16]), rather than the method described in the example of the previous sections. Because Shamir secret sharing is used, M is chosen to be a prime number, say $M = 1009$.

For example, suppose we wish to protect against one device failure and one leaky device; we'll use a PS with four rows and two columns. The votes are $(4, 3)$-shared by in the finite field F_M by the voter Tablet and the shares of each vote are securely sent to four devices $P_{1,1}, \ldots, P_{4,1}$ comprising the first column of the PS. With $(4, 3)$-secret-sharing each value is split into four shares, such that any three (but not any two) suffice to reconstruct the value.

Every first-column Proof Server device $P_{j,1}$ $(4, 3)$-shares the value 0 among the 4 devices in the first column. Every $P_{j,1}$ adds the received shares of 0 to its input share. (This is

done separately for each vote.) The first column devices shuffle the obfuscated quadruples and every $P_{j,1}$ sends its obfuscated share to $P_{j,2}$. The second column of the PS obfuscates and shuffles, produces the results as output.

Now the servers $P_{1,2}$, $P_{2,2}$, $P_{3,2}$, $P_{4,2}$ of the second column each prepares an array of commitments to split value representations of its permuted array of shares of the n vote values w_1 , w_2 , $\ldots w_n$. These commitments are posted on the SBB. This whole process is repeated $2m$ times. Then the m permuted arrays of the (4, 3) shares of the n vote values w_1 , w_2 , $\ldots$, w_n , are posted as in Sections VII–IX.

In general, if at most f devices may fail (where $f > 0$) and at most ℓ may be leaky, then PS may have r rows and c columns, where $r \geq f + \ell + 2$ (to protect votes from leaking), use an $(r, \ell + 2)$ secret-sharing method, and choose $c \geq \ell + 1$ (to protect the shuffles). If $f = 0$, then the number of rows and the number of columns need only be $\ell + 1$, as in the example of the previous sections.

For additional protection against possibly malicious servers, one may for example employ Trusted Platform Module (TPM) technology. Work in progress (to appear) presents additional methods for countering malicious servers who attempt to actively disrupt the protocol. Of course, when paper ballots are available (as with Scantegrity or Star-Vote), one can always recover the correct election outcome by counting them.

XI. Practical Aspects

We consider some practical aspects of the proposed method, such as time and storage requirements.

Assume that the number n of ballots is 10^6, the number of tablets is 10^4, and that we use $2m = 24$. The following numbers are for a typical desktop computer or laptop, which can execute 200 private-key operations (e.g. RSA 2048-bit) per second or 8 million commitments (AES operations) per second. Assume that PS has $r = 3$ rows and $c = 3$ columns.

Time to decrypt votes from tablets: This requires 10^4 private-key operations (using a hybrid method) per first-column PS device—about 50 seconds. It also requires about 10^6 openings of pairs of commitments—under a second. The 50 seconds for the private-key operations is the major component of the running time. The last-column PS devices must prepare 24 arrays of length n with 6 commitments per vote—about 18 seconds (six seconds if the last-column processors do this in parallel). The time to create the random permutations is negligible.

Size of proof: If each commitment $\textsc{Com}(u)$ is assumed to require 30 bytes, then the overall size of the proof is about $25 \times 2 \times 3 \times 30 \times 10^6$ bytes (4.5GB), about the size of a movie; the proof can be downloaded on an typical internet connection in a few minutes at most, and checked in a couple of minutes on a typical laptop.

Code: A 2800-line python program for running simulated elections was written and tested; in experiments it performs flawlessly and rapidly. (See https://github.com/ron-rivest/split-value-voting .)

XII. Conclusion

The methods presented here provide new ways for implementing verifiable mix-nets and thus end-to-end verifiable voting. The new methods are particularly efficient since they do not require any modular exponentiations or public-key operations. We believe that the efficiency and generality of this solution render it practical for actual deployment in elections.

Acknowledgment

We thank Tal Rabin for advice on proactive secret sharing. The second author gratefully acknowledges support from his Vannevar Bush Professorship. We thank the anonymous EVOTE reviewers for numerous constructive suggestions.

References

[1] B. Adida and R. L. Rivest, "Scratch & vote: self-contained paper-based cryptographic voting," in *Proceedings of the 5th ACM workshop on privacy in electronic society*, R. Dingledine and T. Yu, Eds. ACM, 2006, pp. 29–39.

[2] R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Herrnson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora, "Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy," in *Proceedings USENIX Security 2010*, I. Goldberg, Ed. USENIX, August 11-13, 2010.

[3] A. Essex, J. Clark, U. Hengartner, and C. Adams, "Eperio: Mitigating technical complexity in cryptographic election verification," in *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, ser. EVT/WOTE'10. Berkeley, CA, USA: USENIX, 2010, pp. 1–16.

[4] H. Jonker, S. Mauw, and J. Pang, "Privacy and verifiability in voting systems: Methods, developments and trends," Cryptology ePrint Archive, Report 2013/615, 2013.

[5] S. Popoveniuc, J. Kelsey, A. Regenscheid, and P. Vora, "Performance requirements for end-to-end verifiable elections," in *Proceedings of the 2010 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, ser. EVT/WOTE'10. Berkeley, CA, USA: USENIX, 2010, pp. 1–16.

[6] R. J. F. Cramer, M. Franklin, L. A. M. Schoenmakers, and M. Yung, "Multi-authority secret-ballot elections with linear work," Centrum voor Wiskunde en Informatica, Tech. Rep. CS-R9571, 1995.

[7] J. Benaloh, M. Byrne, P. Kortum, N. McBurnett, O. Pereira, P. B. Stark, and D. S. Wallach, "STAR-vote: A secure, transparent, auditable, and reliable voting system," *arXiv preprint arXiv:1211.1904*, 2012.

[8] S. Micali and M. O. Rabin, "Cryptography miracles, secure auctions, matching problem verification," *CACM*, vol. 57, no. 2, pp. 85–93, February 2014.

[9] M. Rabin, R. Servedio, and C. Thorpe, "Highly efficient secrecy-preserving proofs of correctness of computations and applications," in *Proceedings of 22nd IEEE Symposium on Logic in Computer Science*. IEEE, 2007, pp. 63–76.

[10] M. O. Rabin and R. L. Rivest, "Practical end-to-end verifiable voting via split-value representations and randomized partial checking," April 3, 2014, CalTech/MIT Voting Technology Project Working Paper 122.

[11] ——, "Practical provably correct voter privacy protecting end to end voting employing multiparty computations and split value representations of votes," May 12, 2014, CalTech/MIT Voting Technology Project Working Paper 124.

[12] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[13] J. Benaloh, "Ballot casting assurance via voter-initiated poll station auditing," in *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*. USENIX, 2007, p. 14.

[14] C. Cullane and S. Schneider, "Peered bulletin board for robust use in verifiable voting systems," arXiv.org/abs/1401.4151, Jan. 16, 2014.

[15] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Crypto '86*, ser. Lecture Notes in Computer Science, vol. 263. Springer, 1986, pp. 186–194.

[16] R. Ostrovsky and M. Yung, "How to withstand mobile virus attacks," in *Proc. 10th ACM Symp. Princ. Distr. Comp.* ACM, 1991, pp. 51–61.

Pretty Understandable Democracy 2.0

Stephan Neumann, Christian Feier, Perihan Sahin, and Sebastian Fach
Technische Universität Darmstadt / CASED, Germany
Email: stephan.neumann@cased.de, feier@rbg.informatik.tu-darmstadt.de,
perihansahin87@hotmail.com, info@sebastian-fach.de

***Abstract*—Technology is advancing in almost all aspects of our everyday life. One interesting aspect is the possibility to conduct elections over the Internet. However, many proposed Internet voting schemes and systems build on unrealistic assumptions about the trustworthiness of the voting environment and other voter-side assumptions. Code voting – first introduced by Chaum [Cha01] – is one approach that minimizes the voter-side assumptions. The voting scheme Pretty Understandable Democracy [BNOV13] builds on the idea of code voting while it ensures on the server-side an arguably practical security model based on a strict separation of duty, i.e. all security requirements are ensured if any two components do not collaborate in order to violate the corresponding requirement. As code voting and strict separation of duty realizations come along with some challenges (e.g. pre-auditing phase, usability issues, clear APIs), the goal of our research was to implement Pretty Understandable Democracy and run a trial election. This paper reports on necessary refinements of the original scheme, the implementation, and a trial election among the different development teams.**

I. Introduction

The advance of technology, more and more, impacts our everyday life. Shopping, banking, or chatting with friends no longer depends on physical presence but may be easily done independent of time and location by digital means. In recent years, even fundamental processes of democracy have come into the focus of technological advance. Amongst the most attractive options is the possibility to conduct elections over the Internet. Since the seminal work by Chaum [Cha81], many works addressed the challenge of voting over the Internet addressing a broad set of security requirements, see for instance [LSBV10]. It turns out, however, that most of the present schemes rely on unrealistic assumptions to ensure security: for instance, the JCJ [JCJ05] scheme relies on the voter's platform being trustworthy and the Helios voting system [Adi08] relies on the voter conducting a complex verification procedure several times. The number of infected computers[1] shows that it is not realistic to rely on voters to ensure that their platforms are trustworthy. It has also been shown (e.g. in [KOKV11]) that in particular with the Helios voting system, verifiability is not accessible to voters. Furthermore, Olembo et. al [OBV13] have shown that voters do not even see the need to verify their vote due to their trust mental models.

Code voting – first introduced by Chaum [Cha01] – is one approach that minimizes the voter-side assumptions. Since its invention several code voting schemes with different advantages and disadvantages have been proposed [HS07], [JRF09], [RT09]. Recently, Budurushi et al. [BNOV13] proposed a new code voting based Internet voting scheme, Pretty Understandable Democracy (PUD). It ensures an arguably practical security model based on a strict separation of duty, i.e. all security requirements are ensured if any two components do not collaborate in order to violate a corresponding requirement. Furthermore, the authors' goal was to keep the scheme as simple as possible. To date, PUD has not been implemented and therefore has only been considered from a purely theoretical perspective.

Contribution. As code voting and strict separation of duty realizations come along with some challenges for the implementation process, the election preparation and the vote casting (e.g. pre-auditing phase, usability issues, clear APIs), the goal of our research was to implement Pretty Understandable Democracy and run a trial election. In order to implement components by a rigorous separation of duties, we decided to implement components by group-wise student projects within a computer science class at the Technische Universität Darmstadt, Germany. In this paper, we present several improvements and refinements made to the original scheme. Thereafter, we report on our experience about the implementation of the revised scheme and running a trial election among the different development teams (each team being responsible for one component).

Related Work. Chaum's seminal work on code voting [Cha01] has motivated many researchers to build their schemes upon the same idea, e.g. [HS07], [JRF09], [RT09]. The Norwegian Internet voting system [iEGT12] also uses some kind of code voting. While their verification code approach prevents single components from undetectably violating integrity, secrecy builds upon the assumption of a trustworthy voter platform [KLH13]. The only scheme we are aware of following the distribution of trust principle as precisely as PUD is Pretty Good Democracy (PGD) [RT09][2]. As opposed to PGD, PUD is tailored towards understandability and therefore real-world applicability. A more thorough review of the related work can be found in [BNOV13].

PUD in a Nutshell. Code sheets in PUD have three parts: The first part consists of a permuted list of candidates, the second and third parts consist of random and unique codes. The code parts each hold one further code which corresponds to an acknowledgement code. Throughout the code sheet generation, the respective authorities commit on their generated code sheets by encrypting them with an additively homomorphic encryption scheme (in our case ElGamal) and publishing the code sheet parts on a bulletin board. Before randomly

[1] According to [Pan14], in 2013 31.53% of all computers were infected by malware

[2] It should be emphasized that PGD's adversary model is stronger because stored-as-cast integrity can be increased linearly with number of trustees, while PUD allows further conspiracies to violate integrity.

sending out composed code sheets to voters, a fraction of code sheets is audited by comparing the printed code sheets to the encrypted version on the bulletin board. Once, the voter casts the concatenated code (from the second and third code sheet parts) which corresponds to her preferred candidate, the code parts are forwarded to the authorities that generated the respective parts. Given the encryptions of code sheet parts, both authorities are able to re-encrypt the candidate ciphertext that corresponds to that code *without* knowing the candidate within that ciphertext. In the tallying phase, the published candidate re-encryptions are summed up homomorphically and distributively decrypted. By calculating the discrete logarithm, the final result can be obtained. The tallying process is publicly verifiable.

Remark. The full version of this paper [NFSF14] contains an extended introduction to the PUD scheme and all user interfaces. For a detailed review of PUD's security model, we refer the reader to the original PUD publication [BNOV13].

II. Preliminary Setting and Task Organization

Pretty Understandable Democracy (PUD) has been implemented within a student project as part of the lecture *Electronic Voting* in the winter term 2013/14 at the Technische Universität Darmstadt, Germany. Students participating in this course had a background in computer security and cryptography.

1) Pre-considerations: Before the course started, it has been agreed on which parts should be realized and which are not realistic within a course exercise. First, we simplified the authentication step during the election process by simply using the voter's name instead of a strong authentication method. In PUD, any communication between two components is secured by applying TLS. In contrast to a real-world system, the project management team signed the public key for each component and acted as a Certificate Authority. It was decided that the servers did not have to be protected against hackers etc.. In a real-world scenario protection against several threats, like denial of service attacks (DoS), would be necessary but was out of scope for the implementation task. However, this enabled the students to use their own laptops. Motivated by a newspaper report[3] we decided to tailor our trial election towards the *"Bürgerschaftswahl"* (which translates to State Election) of the Hanseatic City of Lübeck and implemented the respective ballot from the last state election. Furthermore, it was decided that $35 - 40$ voters (i.e. all students and supervisors) should be eligible to vote in the trial election at the end of the semester. The software development teams were free to choose any programming language, as long as they were able to provide communication interfaces for the other components. This had several advantages: First, due to the different programming skills within specific languages, students could build upon their preferred languages. Second, relying on one single programming language could result in system vulnerabilities due to the compiler. An adversary could corrupt the whole system by just corrupting the used compiler. By using different programming languages, also different compilers/interpreters are used. For distributed key generation and tallying, we extended an already existing Android application [NKMV13]. We defined a threshold of two out of three.

[3] http://www.segeberger-zeitung.de/Schleswig-Holstein/Landespolitik/Kommunalwahl-2013/Albig-erwaegt-Online-Wahl

2) Organization: There were several software development teams (each one consisted of 2 to 3 students) while each team was assigned to one component and one phase. There were the following software development teams: Voting authorities (*VA1* and *VA2*) *VA1*-setup, *VA1*-voting, *VA2*-setup, *VA2*-voting, *Trustees*-audit, *Trustees*-tallying, the registration authority *RA*-setup, *RA*-voting. In addition, there were the project management team, the bulletin board (*BB*) team, and the distribution authority (*DA*) team. Students in the software development team were explicitly told to not copy any code from other groups to ensure the required separation of duty (SoD).

3) Schedule: The lecture started on October 18, 2013. There were two sessions to discuss the PUD scheme. The group assignment was done afterwards. Correspondingly, the software development part started on November 5th, 2013 and the trial election was scheduled for February 7th, 2014. Thus, the teams had about three months time to implement and test their components.

4) Project management: The software development teams were asked to send their component design, their interfaces and their project schedule until November 15th, 2013 to the project management team. This was done in order to detect and correct design flaws in an early stage of the development process. As target date for the first integration test, the project management team proposed January 15th, 2014. During the development process the software development teams were free to organize themselves, but they were repeatedly asked to report their current status to the project management.

III. Protocol Refinements

After foundational concepts of electronic voting were introduced to the students, there were two lectures on Pretty Understandable Democracy in which the scheme was introduced and discussed with the students. During these discussions, a couple of improvements were identified. These are proposed and discussed in this section.

Candidate encoding. The original proposal was to encode candidates within one single ciphertext. Due to the fact that throughout the tallying process, all encryptions are summed up, each individual encryption of a candidate must also encode *null* encodings of all other candidates. As a consequence, computing the discrete logarithm for such a complex encoding results in a computationally-intensive task even for small-scale elections. Following the multi-candidate punch-hole vector-ballot by Kiayias and Yung [KY04], our revised scheme encodes each candidate into a separate encryption indicating whether the candidate is selected or not. Therefore C encrypted blocks are sent where C is the number of candidates. Each block has the form $\{g^x\}^r_{pk_T}$ where r is a random number and x is the number of votes for this candidate. If the voter has exactly one vote this is either 1 or 0. For example there are 3 candidates and the voter votes for candidate 1 and 3. The corresponding encodings are (g^1, g^0, g^1) and the respective encryptions are given as $(\{g^1\}^{r_1}_{pk_T}, \{g^0\}^{r_2}_{pk_T}, \{g^3\}^{r_3}_{pk_T})$. Due to this improvement the necessary number of re-encryptions is increased to C for each voter. Furthermore during the tallying process $2 \cdot C$ homomorphic sums are calculated. To overcome these drawbacks compared to the encoding in [BNOV13] the tallying performance is improved. The encrypted homomorphic sums for each candidate are given as $g^{c_1}, g^{c_2}, ..., g^{c_n}$

where c_i describes the number of votes for candidate i. To solve g^{c_i} the discrete logarithm problem has to be solved but the number of necessary modular exponentiations to find all c_i is limited to $\sum_{i=1}^{C} c_i \leq V$ modular exponentiations where V is the number of eligible voters. This is solvable by using brute-force. Compared to up to $V \cdot 10^{(C-1)\cdot\lceil\log_{10}(V)\rceil}$ modular exponentiations which are necessary to tally as described in [BNOV13] this is a significant improvement.

Cross-checking indices and positions. Originally, PUD prescribed the following procedure: After *RA* split the voting code apart and forwarded the respective parts to *VA1* and *VA2*, *VA1* and *VA2* independently re-encrypt the ciphertext related to the specific voting code (over index and position of the voting code). It turns out that a malicious voter might however prevent the computation of an election result by submitting code parts that represent different candidates, e.g. on the middle code sheet part, the voter would chose the code at position 3 and at the right code sheet part, the voter chooses the code at position 4. In such a case, *VA1* and *VA2* would re-encrypt different candidates and the computed homomorphic sum of both authorities would differ. Therefore, in addition to validity checks, *VA1* and *VA2* cross-check that they obtained codes of the same index and the same position. In case the code is invalid or a mismatch is detected, *VA1* and *VA2* log the corresponding request and inform *RA* that informs the voter.

Code length. The PUD scheme builds upon the use of voting codes to ensure the conduct of secure elections. The length of these codes plays a substantial role to the scheme because it directly impacts security and usability of the scheme. In the final part of this section, we therefore analyze which length voting codes shall have. In order to have unique codes, for C candidates and V voters, there are at least $(C+1)\cdot V$ codes per *VA* required. To allow a sufficient proportion of the code sheets to be randomly audited, a factor λ is used. Therefore $\lambda\cdot(C+1)\cdot V$ codes are needed for each *VA*. Furthermore, the codes generated by *VA1* and *VA2* are disjoint which results in a factor 2 of generated codes. Therefore $2\cdot\lambda\cdot(C+1)\cdot V$ codes are needed for both *VA*s. This means that $\log_2(2\cdot\lambda\cdot(C+1)\cdot V)$ bits are necessary for each code to ensure that all codes are different. For the trial election, we set $\lambda = 2$. With `Base32` encoding, each code consists of 3 characters.

IV. Implementation

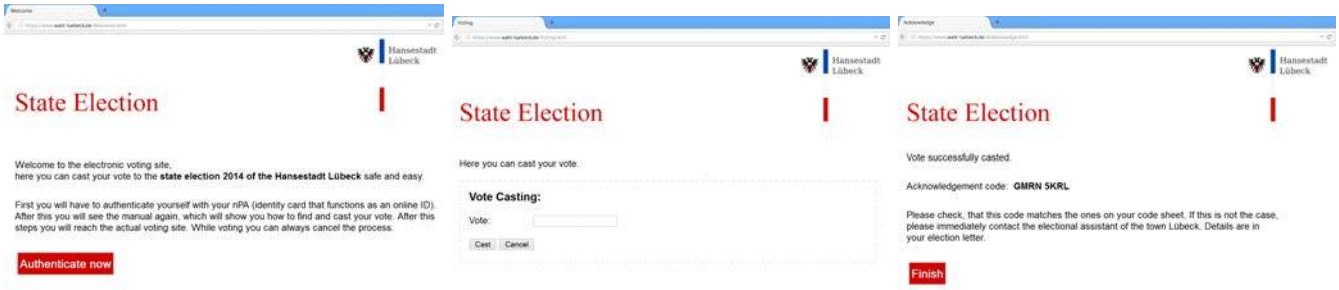
Programming Languages and Programming Interfaces. The development teams agreed on Python, Java and Scala as programming languages. Both parts of *RA* and *BB* are written in Python, both parts of *VA1* and *VA2* are written in Java and the *DA* is written in Scala. In order to ensure a smooth communication between the involved entities, the students agreed on a REST API to receive and send data. To publish the specific syntax for each command an internal Wiki was used in which each team documented all available commands for their API. Some students did never work with a REST API and had to start learning it first.

Election Material and User Interfaces. The election materials as well as the user interfaces were developed in an iterative process, i.e. members of different teams provided feedback as well as friends not being involved in the process. The election material was developed by the *DA* team in close collaboration with the *RA*-voting team. Once visited the election website, information about the Internet voting process is displayed (see Figure 1(a)). In order to proceed, the voter needs to click on 'Authenticate now'. The voter, then, authenticates himself/herself. After being authenticated, the next interface displays the election manual (similar to the election material received together with the code sheets). The voter continues by clicking on 'Vote now'. The system re-directs the voter to the next interface on which he/she casts his/her vote (Figure 1(b)). Both codes of his/her preferred candidate need to be provided in the field next to 'Vote'. Spaces will be deleted by the interface. The vote casting can either be completed by clicking on 'cast' or canceled. Once cast, the interface displays the information that the vote has been successfully cast and the respective acknowledgement code as shown in Figure 1(c). The BB provides different sectors for all phases of the election process. Every entity has read access and except the Distribution Authority also write access. All data published on the Bulletin Board is signed by the publishing authority. For example, throughout the setup phase, commitments of code sheets are published on the BB

Tests. To test their components the teams wrote their own test cases. Unfortunately, some teams did not stick to the plan on the first test, which was as announced on January 15th. Therefore, the final complete test took place at February 6th, 2014, only one day before the trial election. At the final test some problems occurred, which had to be fixed: The communication from any component to *VA1* did not work because of a TLS error. Furthermore the tallying module did not work correctly because the group did not implement homomorphic tallying properly. To fix these problems, the students worked until late night and the whole morning before the trial election. This experience shows that time schedules are even more important if (voting) systems are developed in a distributed manner.

V. Lessons Learned

The trial election was conducted on February 7th, 2014. Assembling all the needed papers (three code sheets and the election manual) took about 20 minutes (with one printer) for the small trial election with 50 voters, where ten persons in parallel took care of preparing the voting papers. This process could possibly be improved by special machines. Even without machines, the process could be organized in a way that is acceptable as in many German cities the postal voting material is also prepared manually. Auditing only five code sheets took us more than 10 minutes. It just takes time to open the envelopes and read aloud all the candidates, then all the codes from *VA1* and then all the codes from *VA2* for each audited code sheet. It even takes more time, if this is done in a transparent manner, i.e. the present observers can follow the process. When entering the codes, we noticed that some participants were confused by entering both parts of the code in the same text field. It might be worth providing two different fields in future and clearly indicating which code to enter in which field. The different views of the bulletin board were clear to the participants. However, it was also discussed that in case - due to transparency requirements - it is assumed that also voters should understand the content of the bulletin board, further information needs to be provided.



(a) Welcome Interface. (b) Vote casting interface. (c) Interface with acknowledgment.

Fig. 1. User-interface

VI. Conclusion

The present work reports about the experience of refining and implementing Pretty Understandable Democracy (PUD) and running a trial election with that scheme as part of a computer science course. The insights gained throughout the implementation and the trial election process are manifold and serve as guidelines for future research. PUD has been introduced as a theoretical concept and as such several details remained open. This gap forms the motivation for the present work. The first refinement is the multiple ciphertext encoding of single votes, which reduces the number of modular exponentiations needed throughout the tallying process significantly. In order to prevent malicious voters from blocking the calculation of the election result, the voting authorities cross-check the consistency of voting codes. Furthermore, we analyzed the required lengths of voting for different election settings. Finally, in order to conduct the trial election as close as possible to real-world elections, we proposed user interfaces tailored towards the state election of the Hanseatic city of Lübeck which currently considers introducing Internet voting. The contributions of this work builds *one* step towards PUD's real-world applicability knowing that there are many challenges open challenges before its first usage. Throughout the trial election, individual code sheet parts had to be combined into one envelope and sent out to voters. This results in significant organizational and time-intensive effort. We consider revising the code sheet distribution process, thereby lowering the organizational effort. Discussions among the students and the staff show that from a usability perspective the scheme is going into the right direction. In order to evaluate the scheme's usability in an unbiased manner, user studies will be conducted in the near future. PUD has been tailored towards a trade-off between security and transparency. Nevertheless, the scheme builds upon several cryptographic primitives. We plan to investigate the scheme's understandability by preparing information and education material and evaluating it in user-studies.

Acknowledgment. This work has been developed within the project ComVote, which is funded by CASED.

References

[Adi08] Ben Adida. Helios: Web-based open-audit voting. In Paul C. van Oorschot, editor, *USENIX Security Symposium*, pages 335–348. USENIX Association, 2008.

[BNOV13] Jurlind Budurushi, Stephan Neumann, Maina Olembo, and Melanie Volkamer. Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme. In *8th International Conference on Availability, Reliability and Security*, pages 198–207. IEEE, 2013.

[Cha81] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[Cha01] David Chaum. Sure vote: Technical overview. In *Proceedings of the Workshop on Trustworthy Elections (WOTE 01)*, 2001.

[HS07] Jörg Helbach and Jörg Schwenk. Secure Internet Voting with Code Sheets. In *VOTE-ID*, pages 166–177, 2007.

[iEGT12] Jordi Barrat i Esteve, Ben Goldsmith, and John Turner. International experience with e-voting. 2012.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *ACM Workshop on Privacy in the Electronic Society*, pages 61–70. ACM, 2005.

[JRF09] Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira. VeryVote: A Voter Verifiable Code Voting System. In *Proceedings of the 2nd International Conference on E-Voting and Identity*, VOTE-ID '09, pages 106–121. Springer-Verlag, 2009.

[KLH13] Reto E Koenig, Philipp Locher, and Rolf Haenni. Attacking the verification code mechanism in the norwegian internet voting system. In *E-Voting and Identify*, pages 76–92. Springer, 2013.

[KOKV11] Fatih Karayumak, Maina Olembo, Michaela Kauer, and Melanie Volkamer. Usability analysis of helios - an open source verifiable remote electronic voting system. In *Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*, 2011.

[KY04] Aggelos Kiayias and Moti Yung. The vector-ballot e-voting approach. In *Financial Cryptography*, pages 72–89. Springer, 2004.

[LSBV10] Lucie Langer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer. A taxonomy refining the security requirements for electronic voting: analyzing helios as a proof of concept. In *5th International Conference on Availability, Reliability and Security*, pages 475–480. IEEE, 2010.

[NFSF14] Stephan Neumann, Christian Feier, Perihan Sahin, and Sebastian Fach. Pretty understandable democracy 2.0. Cryptology ePrint Archive, Report 2014/625, 2014. http://eprint.iacr.org/.

[NKMV13] Stephan Neumann, Oksana Kulyk, Lulzim Murati, and Melanie Volkamer. Towards a practical mobile application for election authorities (demo). In *4th International Conference on e-Voting and Identity (VoteID13)*, 2013.

[OBV13] Maina M. Olembo, Steffen Bartsch, and Melanie Volkamer. Mental models of verifiability in voting. In *Proceedings of the 4th International Conference on E-Voting and Identity*, VoteID'13, pages 142–155, Berlin, 2013. Springer-Verlag.

[Pan14] Panda Security. Annual Report Pandalabs 2013 summary. http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report_2013.pdf, 2014. Online; accessed 30 May, 2014.

[RT09] Peter Y. A. Ryan and Vanessa Teague. Pretty Good Democracy. In Bruce Christianson, James A. Malcolm, Vashek Matyas, and Michael Roe, editors, *Security Protocols Workshop*, pages 111–130. Springer, 2009.

Trust in Electronic Voting

Trust in Internet Election Observing the Norwegian Decryption and Counting Ceremony

Randi Markussen, Lorena Ronquillo and Carsten Schürmann
IT University of Copenhagen. Rued Langgaards Vej 7
DK-2300, Copenhagen (Denmark)
Email: {rmar, lron, carsten}@itu.dk

***Abstract*—This paper discusses the Decryption and Counting Ceremony held in conjunction with the internet voting trial on election day in the Ministry of Local Government and Regional Development of Norway in 2013. We examine the organizers' ambition of making the decryption and counting of electronic votes public in order to sustain trust in internet voting. We introduce a pragmatic approach to trust that emphasises the inseparability of truth from witnessing it. Based on this and on a description of how the event was made observable and how the complexities in the counting process were disclosed, we discuss what we term *economy of truth* from the perspective of the IT community involved in the ceremony. We claim that broadening the economy of truth by including more explicitly social and political perspectives in the ceremony, and in internet elections in general, and how witnessing is brought about, would make a more solid case for understanding how democracy is transformed.**

I. Introduction

Democratic elections in contemporary society, according to Article 21, Universal Declaration of Human Rights, shall be periodic and genuine; they shall be by universal and equal suffrage and guarantee the secrecy of the vote. Practicing elections in a manner that is compatible with these principles raises, among other things, the question of who is involved in organising, administrating and overseeing the electoral process and the voting procedures, in particular. Thus the public staging of the election, as well as public involvement in the counting, have in many countries been constitutive elements in preserving trust and legitimising a representative democracy.

Internet voting challenges these elements in a significant and profound manner, as the public engagement in counting is replaced by counting by computers that are managed by technical experts. What is rarely addressed in detail, however, is how the experts carry out their work, and how their activities may relate to the public. The internet voting trials in Norway in 2011 [2], [19], [29] and in 2013 [7], [22] stand out, as the Norwegian Ministry deliberately experimented with the idea of publicly overseeing the experts' counting activities during a public event, the so-called Decryption and Counting Ceremony. The Ministry of Local Government and Regional Development of Norway (hereafter *the Ministry*) was responsible for designing and running the ceremony. The ceremony took place on the premises of the Ministry on election day.

In this paper, we study in detail the way in which the Administration Board (employed by the Ministry) rendered the decryption and counting activities observable. The goal of the ceremony was to convince the audience that truth is produced. The Ministry argued in advance that "Observation in the *back office* combined with voter observation of return code replaces the function of the observer in the polling station" [6]. We mainly concentrate on the *back office* disclosure in order to explore how the idea of trust in this event can be addressed.

Based on a pragmatic understanding of trust in science and within science, and inspired by Shapin's framework [26, p. 6], we describe the ceremony and explore what we term *economy of truth* from the IT community's perspective. We argue that broadening the economy of truth by articulating more explicitly social and political perspectives may create a more solid understanding of how democracy is transformed. Our arguments intend to inform research communities in the area of e-governance more broadly, when trust is a key concept, as well as politicians and the public in general.

This paper is organized as follows: Section II introduces a pragmatic, philosophically motivated understanding of trust and its importance in everyday life as well as in scientific communities, and briefly presents its relevance in understanding trust in elections. Section III introduces the Decryption and Counting Ceremony and its organizational set up, including the legal bodies witnessing the event. Then, Section IV gives a high-level understanding of the decryption and counting stages of the Norwegian internet voting system as it was designed, and sketches those procedures that were executed during the actual ceremony to render parts of the system observable. The description aims by no means at being a comprehensive outline of all the details involved in the ceremony, but it serves mainly to communicate the technical complexities and challenges involved in the ceremony in a manner that is consistent with what the organizers probably intended to achieve. More technical information about the voting protocol can be found in [11]. Section V brings the insights from the various sections together by discussing the economy of truth shaped by the Decryption and Counting Ceremony from a technical perspective, as well as a social and political perspective, and finally Section VI concludes the paper.

II. How to understand trust

Over the last decades the term *trust* has received increasing academic attention. This is driven in part by our curiosity to understand how contemporary societies work, not least the role of trust in science in the making of society, as well

as the role of trust in producing knowledge within scientific communities [15], [27], [33]. Predominant perspectives tend to build on rational philosophical assumptions focusing on individual rational decision making. In contrast, pragmatic perspectives, which are the ones this paper follows, emphasize the collective aspects in the making of social orders and in knowledge production, and argue that whether actions are rational or not do not belong to the individual actor, but it also depends on how they are perceived by others [30, p. 19]. Of special interest in our context is Steven Shapin's seminal work on the origins of experimental philosophy [26]. Shapin shows that the gentlemanly culture of truth telling that Robert Boyle together with members of the Royal Society developed was consequential for trust in their new natural science. Furthermore he suggests that contemporary scientific truth claims similarly involve the witnessing by specific scientific communities [26]. In relation to elections, this argument implies that the community involved in the counting go hand in hand with the community of accounting. Where Besselaar et al. [5] argue that voters' trust in the technology is more important than the technical characteristics, we want to avoid in this paper the dichotomy between trust/subjectivity versus things/objectivity and argue that the concept of technical characteristics is closely related to the witnessing of truth claims within a specific scientific community.

Thus trust is involved in the dynamics in social ordering in everyday life, as well as in scientific knowledge production, as no single individual can constitute knowledge outside of a community. "Truth consists of the actions taken by practical communities to make the idea true, to make it agree with reality" [26, p. 6]. Shapin stresses that pragmatic philosophers reject a static understanding of truth, and emphasises the close connection between truth and trust by pointing to their etymological root in the Germanic word for tree: "Trust/truth is therefore, like a tree, something to be relied upon, something which is durable, which resists, and will support you." [26, p. 20]. The early pragmatist philosopher W. James compared the investment in trust to a credit system: "Our thoughts and beliefs *pass*, so long as nothing challenges them, just as bank-notes pass as long as nobody refuses them." [13, p. 88-91]. In connection to elections, this argument suggests that if people experience their government to be well working and find elections are held and have been held in a fair manner, they will continue trusting it until an event proves this wrong. The recent evaluation report of the Norwegian internet trial in 2013 [24] also makes this argument, suggesting that the slight reduction in trust in elections which was perceived in the municipalities involved in the internet election in 2011 had to do with its newness. But the moment people did not experience any major public scandals, the level of trust was reestablished [24].

This illustrates that trust not only involves routine interactions, it includes deliberate decisions on whether to trust or not, as well as distrust and scepticism. Trust but also distrust "presuppose a system of takings-for-granted which make this instance of distrust possible." [13, p. 19]. Thus computer scientists, especially cryptographers, share by training a specific way of addressing a situation and discussing the relevance of specific arguments. Hence the character of scepticism depends upon the extent and quality of trust in a given community. In a Scandinavian context it is often said that people trust their governments[1], meaning that if people express scepticism and distrust, it should be seen against a solid quality of trust as well. Scientific communities, or political communities to mention some, may cultivate specific language games, ways of making truth claims and discussing them. The opposite of trust in Shapin's account is "the public withdrawal of trust in another's access to the world and in another's moral commitment to speaking the truth about it (. . .). It is not just that we do not agree with them; it is that we have withdrawn the possibility of disagreeing with them." [26]. Thus trust, as well as distrust, are involved in making democratic societies work, and without them societies may fall apart.

We are especially interested in the metaphor of *economy of truth* that Shapin shortly introduces: "Knowledge is the result of the community's evaluations and actions, and it is entrenched through the integration of claims about the world into the community's institutionalized behavior. Since the acts of knowledge-making and knowledge protecting capture so much of communal life, communities may be effectively described through their economies of truth." [26, p. 6]. The metaphor *economy* suggests that there are interests, costs, and values involved in truth-making and hence trust-making, and that protecting certain ways of understanding the world, may be as important as producing knowledge. For instance, an economy of truth shaped by paper ballots and public involvement, is extraordinary in that it consists of all voters, including election officials who know the regulations and procedures. They perform a temporary community, distributed into several minor communities all over the countries, who have to contrive to work together locally and apply the regulations in practice. More can be said about how computers are already applied in many of their work activities. Suffice to say that the process is nonetheless in economic terms sometimes described as *people intensive* as opposed to technology intensive, following a dominant logic in our economy of replacing human labour with machines. In our context, internet voting as well as e-voting involve new scientific communities of knowledge-making and consequently other aspects of the economy of truth. Indeed, they require new equipment and machines, which in Shapin's argument, depend on specialized knowledge and a community that favours specific truth claims and ways of producing and protecting truth, as we explore in this paper. One may talk, for instance, about an economy whose monetary units includes competences, truth claims and ways of dealing with them, technologies, proofs, etc.

An important instrument for maintaining confidence in the electoral process and giving elections credibility is often expressed as transparency in every step [8], [32], meaning that the government and the organizers do not hide activities from the public. Practicing elections along these principles is a well-established habit in Norway and has no doubt inspired the Norwegian Ministry in organising the ceremony and trying to create a public space to attest to the truth produced in the counting of internet votes.

[1] According to the OECD's Better Life Index [20], 66% of people in Norway say they trust their national government, being one of the highest rates in the OECD and much higher than the OECD average of 39%.

III. The Decryption Ceremony

In June 2013 the Ministry appointed an Internet Election Committee (IEC), to ensure that the internet voting trial was conducted in accordance with the regulations, and in a manner that is open and the voters could trust [16]. The idea was to have a group of people, independent of the Ministry, to supervise the preparation, conduct verification and approve the results, besides having the authority to suspend or cancel the trial in case of irregularities. The members of this committee were also involved in the decryption event, as we will later see. The nine members covered technical and political competences, and also included a representation from the municipalities involved in the trial: one member from the Norwegian Data Protection Inspectorate, an election researcher, a cryptographer, the chairmen of the Election Boards of three of the counties, and three regular voters selected from the pilot municipalities [16]. In addition, a verification team consisting of three people with electoral and technological expertise was appointed to check the correct behaviour of the decryption and counting process [22].

The composition of the new legal institutions is noteworthy, as it suggests that political and social competences are also important in accounting for the event, besides only technical expertise. At the same time, the internet voting technology in use is based on a specialized discourse of advanced mathematics, including cryptography, and its own system of takings-for-granted, assumptions and technical challenges. Opening this black-box to convince the technically savvy audience that the system performs as expected is one thing. However, making specialized concepts such as encryption and decryption keys, secret-sharing and zero-knowledge proofs comprehensible, and therefore relevant, to a public in general that does not necessarily share this discourse, is another.

As already mentioned, many internet voting technologies are based on cryptography, and so is the Norwegian that uses, in particular, asymmetric key cryptography. During the course of the election a public and a private keys are created and used. The public key is known by everyone and used by the voter to encrypt his/her vote and make it unreadable[2], while the private key allows to decrypt the encrypted vote and hence recover the original vote. Clearly, the election private key is of special importance in the voting system when securing the privacy of votes, thus in the Norwegian context the IEC members were assigned the authority to safeguard that key. At the beginning of the election, during the so-called Key Generation Ceremony, the election keys were created and each IEC member was given a smartcard containing a unique share of the private key. Their task consisted of keeping these shares safe until the Decryption and Counting Ceremony, at the end of the election, where by putting at least 6 out of the 9 shares together [14], the key would be reconstructed and used to decrypt the electronic votes.

The Decryption and Counting Ceremony took place in an auditorium in the Ministry, two hours before the election closed. As the design of the auditorium suggests, it creates a room for an audience to watch a performance. In this context, the stage (see Fig. 1) allowed for several computers, a safety deposit box, a blender (used to destroy physical storage media) and some screens, as well as the people responsible for the internet voting system. Besides the IEC and the verifier team, the audience included election observers such as representatives from the OSCE, the Carter Center, as well as from other countries, and also the company that had built the system.

Fig. 1. The setup and the agenda [17].

The term *ceremony* underlines the formal character of a public event, and stresses the serious challenges involved in developing ways of making decryption visible, even to a mixed audience, including anybody interested in watching the online broadcast of the event [17]. However, what is shown in the ceremony is not the final counting of the election results, but a preliminary counting. As mentioned by the main spokesperson, the ceremony works as a *guided tour*, a demonstration of the virtual procedures that describe the internet counting, at the same time as the audience is invited to stay and review the final count later on.

Norway is not the only country in the world having engaged in internet elections. In Estonia, internet voting has been used for binding political elections since 2005, both local and nationwide, and other countries like Canada and Switzerland from 2003, and Australia from 2011 [2], [4] have also used it for some municipalities. However, to our knowledge, the decryption events of these elections, if any, have mostly gone unnoticed in the literature. In the case of Norway, recent reports from International Election Observation Bodies [7], [22] mention the Counting and Decryption Ceremony just as one more step taken by the Norwegian Ministry in order to make the system transparent, but do not seem to have looked into the event as such. In Estonia, Alvarez et al. [1] mention that the decryption and counting of internet votes in the election of 2007 took place before the election closed, and in order to ensure that none of the results from the internet vote tabulation could be broadcast to the media, candidates, or parties until the polls had closed, all communication devices of observers were confiscated, the doors of the room sealed, and security guards posted at the doors, while the authors do not mention any online broadcast of the event. According to the OSCE/ODIHR [21], the counting of internet votes in the Estonian parliamentary elections of March 2011 was done in the presence of the National Electoral Committee members and domestic as well as international observers, but no ceremony, as in the case of Norway, is mentioned either. In the local

[2]This encrypted vote is unreadable under certain assumptions well-known within the cryptographic community but out of the scope of this paper.

elections of October 2013, however, Halderman et al. [12] do mention in passing that the encrypted votes were decrypted and counted at an event that resembles somewhat the Norwegian Decryption and Counting Ceremony, in that there was an audience witnessing the process in a room of the Estonian Parliament building, and the event was also made available online [10]. As for other countries like Canada, Switzerland, and Australia, to our knowledge, the opening of the electronic ballot box and decryption of internet votes was not witnessed by the public, but by scrutineers and sometimes also the police, as in the case of Geneva, Switzerland.

IV. Decryption and counting

This section briefly describes the main characteristics of the Norwegian internet voting system, paying special attention to the decryption and counting stages, and then reviews some of the procedures we observed about the system working during the public ceremony.

The Norwegian internet voting system is conceived as a supplement of the traditional paper-based voting. In order to mitigate the risk of voter coercion or vote buying inherent to internet voting, and given that voters were able to vote electronically during an advance voting period of roughly one month, the system supports *repeat voting*, by which voters are able to vote multiple times, but in such a manner that only one vote will be counted. Thus if a voter casts multiple electronic ballots, the last cast ballot is the one counted, while any vote cast on paper is final and overrides previous electronic votes [11].

The system also uses return-codes, a mechanism that allows voters verify that their vote has been correctly received by the voting server and thus provides individual verifiability, usually referred to as *cast-as-intended*. This feature is not discussed further in this paper.

An important cryptographic component of the Norwegian internet voting system are *zero-knowledge proofs*, i.e. methods by which a verifier can be convinced (with negligible amounts of doubt) that a particular statement is true without learning anything else apart from the fact that the statement is true. In the case of voting, for instance, zero-knowledge proofs allow verifiers to check, among other things, that the votes have been correctly decrypted without the private key being revealed to them.

The electronic ballot box contains all internet ballots encrypted [9] and also digitally signed by the corresponding voter [11]. Once the voting phase is over, this ballot box is taken offline and handled on air gapped servers, i.e. physically isolated and not connected to the internet. The decryption and counting of internet votes thus takes place in three phases. The first phase, called *cleansing*, identifies the ballots that will be counted according to the repeat voting policy, and disregards the rest. The signature of the resulting ballots is also checked during this phase. The second phase is called *mixing*, which cryptographically anonymizes the cleansed ballots so as to prevent tracing them back to the voters who cast them. This means that the ballots are shuffled and re-encrypted at each mix-net node, so that they end up in a different order and also look different (yet still encrypt the same votes). In the final phase, the *e-counting*, the decryption key is recovered from the shares of the smartcards of the IEC [25]. The mixed ballots are then decrypted, tallied, and the electronic vote count is finally submitted to the central election administration system (EVA[3]).

In addition, every phase of the decryption and counting process generates zero-knowledge proofs showing, respectively, that the cleansing of ballots was done properly, the mix-net nodes behaved correctly and actually shuffled and re-encrypted the ballots, and that the decrypted votes accurately reflect the encrypted votes.

A. Making the decryption and counting visible

In what follows we review some of the relevant procedures we observed, carried out by the Administration Board (hereafter *the organizers*) at the Decryption and Counting Ceremony.

On the auditorium stage there is a table with three laptops, a safety deposit box, a blender and three overhead displays, showing the screen content of the laptop in use, as well as some explanatory slides giving details about what is happening during each phase. Two of the organizers are seated at the table. They will be the ones running a number of commands on the laptop corresponding to the respective phase, while a third, the spokesperson, is standing up and guides the event. In a corner of the room, a group of verifiers with a computer connected to their own big screen are sitting and waiting to come into play (see Fig. 1). Among the audience, the nine members of the IEC, equipped with their smartcards, also observe the event, awaiting to be called upon during the e-counting phase to insert their smartcards into a smartcard reader, used to reconstruct the election private key.

According to the organizers, the electronic ballot box that is about to be decrypted and counted as part of the ceremony was retrieved from the central database server some time before the ceremony in the presence of the verification team and the observers. Starting with a memory stick containing the electronic ballot box, a second one containing the electoral roll, and a third one with some other election data, the process goes through the cleansing, mixing and e-counting phases. At the same time, the overhead screens show the commands running each phase. Most of these commands are standard Linux commands, and no user interface is used but the terminal. By doing this, the organizers deliberately give the audience a glimpse into the inner details of the decryption and counting process like, for instance, which folders are being accessed at any time, what is their content, etc.

The three laptops on the table are color-coded and each connected to different servers through a cable of the same color. The audience is informed that each laptop runs one of the three phases of the decryption and counting process, thus the colors identify the components that are in use during each phase, and illustrate that the servers are apparently not connected to each other and therefore are air gapped. To confirm the latter, whenever some data (the processed ballot box) needs to be transferred from one phase to the next one, it is physically moved from one laptop to the one running the next phase by means of a new and recently unsealed memory

[3]Elektronisk Valgadministrasjonssystem.

Fig. 2. A member of the verification team taking a picture of the hash value shown in one of the big screens [17].

stick. These memory sticks are taken from the safety deposit box, for which the verifier team has the key. The organizers also show that the memory sticks are new by showing each time that they are empty. In addition, the main table of the auditorium is *kept tidy* at all times which is achieved by extracting the memory stick from the respective laptop whenever the organizers finish working with it. This aims to help the verification team and the audience to understand the movement of the data throughout the three phases. Furthermore, in order to show that the cleansed ballot box and the mixed ballot box remain unchanged when transferred from one phase to the other, and no process injects new votes into the ballot box, a well-known cryptographic tool known as *hash function* is used. The output of a hash function is unique (at least for our purposes it may be considered as such), thus it is used here to prove the equality of two files located in different machines. In the context of the ceremony, the hash value of the file to be transferred is shown both before being copied to the memory stick, and after being copied to the next machine. This enables the verifier team, as well as anyone among the audience, to take a picture of the first hash value and compare it to the second one for equality (see Fig. 2).

Because of the sensitive nature of the data contained in the two memory sticks used between the cleansing and the mixing phases, and between the mixing and the e-counting phases, as well as to illustrate that the ballots in these memory sticks should never be recovered, these memory sticks are immediately destroyed in a blender after use.

Once the mixing phase is completed, the verifier team is given two memory sticks containing, respectively, the mixed ballot box and the zero-knowledge proofs generated in the mixing phase, to check that the mixing has been conducted correctly. Later on in the ceremony, the verifiers inform that the checking has been successful. Next, as part of the e-counting phase, the organizers take a top hat in which, prior to the ceremony, they have put the name of the IEC members in small pieces of paper. One by one, the members are named at random to bring their smartcards and enter their parts of the key into the system [25], until the election private key can be recovered and finally used to decrypt the internet ballots and obtain the preliminary results. These results are then copied to a memory stick, and transferred to EVA after the public ceremony.

Finally, the verifier team is given the memory sticks containing the mixed ballot box and the zero-knowledge proofs generated in the e-counting phase, to check the decryption. The result of this check, however, is not given during the ceremony because of timing constraints.

V. Discussion

The Decryption and Counting Ceremony demonstrates that the truth in the processes involved in counting electronic votes, when internet is used to cast votes and cryptography is a prime warrantor of both the secrecy of these votes and the election's integrity, is produced very differently from the counting of paper ballots. The sketch in Section IV-A, done primarily with an eye on what we think the intention of the organizers was, points to the event as a spectacle where various elements are visualised in order to make the procedures transparent and observable to the audience and some sort of public. Following Shapin's argument that truth and trust are closely related to the witnessing of an event, we discuss the economy of truth and the ambition of accounting for the decryption to the public in various perspectives on the event.

A. The economy of truth in the IT community's perspective

Trust in the internet election, and in e-voting more generally, is mostly addressed as a question of citizens' trust. Thus the Norwegian evaluation reports of the internet voting trial in 2011 [23, p. 63] and in 2013 [24] measure the degree to which citizens trusted the technology without addressing more explicitly the ceremony and the Ministry's communication efforts as such. More broadly, the field of *e-governance* is engaged in suggesting and defining measures that should be in place for a specific technological solution to be considered trustworthy by the IT community and consequently, as we tend to hope, also by the public. E-governance also focuses on aspects that are relevant to internet voting, such as transparency, evaluation according to international standards, separation of duty, verifiability, vote updating, etc. to establish trust among the public [28], [31].

The Norwegian Decryption and Counting Ceremony adds an important element to this context, however, by opening the black-box of how decryption works, and highlighting that trust as understood by Shapin is an element within the IT community as well. As mentioned in Section II, the IT community shares a system of takings-for-granted that makes them expect certain things to take place, and this in turn makes specific ways of distrusting possible. Indeed, distrust is a hallmark of IT security with its focus on defining adversary models and estimating what might go wrong. As Shapin suggests [26], distrust is crucial in many kinds of knowledge production, and in our view the ceremony points to important aspects of the economy of truth within the IT community. Most importantly, it bears witness to the technical complexity of the Norwegian internet voting system. The IT community seems to agree that this complexity inevitably makes the system prone to risk and failures, as also mentioned in the Carter Center report [7], but it also recognises the efforts made by the organizers in managing the complexity by encouraging transparency and inviting peers to give feedback and witness the ceremony.

The ceremony attests to the idea that IT is not so much an autonomous object as a socio-technical learning process.

However, not everything that the IT community would have liked to observe, could be made visible at the ceremony. For instance, the audience could not check, and therefore needs to trust, that the correct electronic ballot box was the one used for the ceremony, or that the actual preliminary results, and no others, were transferred to EVA. While disclosing these steps could have helped in making the process more transparent, they were only shown to the verifier team. In addition to this, given that the decryption key was recovered from the IEC members during the preliminary count and before the final count, the audience has again to trust the organizers to have safeguarded and not misused it during this (even if short) period of time.

There are some other aspects in which the ceremony, probably due to time or space constraints, did not succeed in making the process more visible from a technical point of view. For instance, the use of standard Linux commands might not have given enough confidence to an IT literate about what the programs were actually doing, since it is possible to override these commands to perform a completely different task. We suspect that before the ceremony started and in front of the verifier team and the observers the organizers demonstrated the robustness of the Linux platform and that they had the right implementation of the hash function. Regarding the zero-knowledge proofs, the public has to trust the verifiers to use reliable software to check these proofs and complete checking those proofs that were not checked by the end of the ceremony. And ultimately, taking into account that what was covered by the ceremony was just a preliminary count, one wonders how the audience can be sure that the final count was indeed done in a manner similar to the simulation just observed. Besides these questions closely related to the system of takings-for-granted in the IT community, one can add the trust in the wider infrastructure in which the internet election and the ceremony depend on. Perhaps not intended as such, but to us, the top hat pointed to the ambiguities involved in keeping some things secret while making others visible, suggesting that the boundaries between science and fiction may not be necessarily as robust as we tend to think.

The organizers took also some other precautions to make the system more transparent, such as, for example, publishing the source code and the system documents in advance. This allowed for independent reviews and assessments and thus contributed to the IT community's trust in the system. The Decryption and Counting Ceremony did this to a much lesser extent because, we suspect, of those aspects that could not made visible during the event, as we have discussed above. More importantly, while the ambition to create transparency is one of the goals of the ceremony, we observe that it is reduced to trusting the work of the verification team that is responsible for approving the final result. Their position in the room as partly on the scene when checking the hashes and equipped with their own computer, and partly in the audience when they sit back and watch together with the rest of the audience, points to their role as what is increasingly termed a *proxy* in the election observation community: a stand in for the audience and the public, as the IEC appointed them. Thus the ceremony makes obvious that trust in that the votes are counted correctly ultimately is about trust in the verifiers, as well as the organizers. In this respect the ceremony relates to the idea of replacing the function of the observer in the polling station in democratic elections.

B. The economy of truth in a social and political perspective

While the ceremony makes it possible for the IT community to discuss and form an opinion on the quality of the counting of votes, it is less obvious, however, to what extent the fact of replacing the observer in the polling station is meant to be an explicit part of the ceremony. One might expect that the IEC was assigned the task to try to address questions relating to democratic legitimacy and political and social aspects of the ceremony and the internet voting trial. But their role in the decryption ceremony was apparently to focus on controlling the access to the election private key, and thus attesting to the correctness of a central albeit small part of the ceremony. They seem to fulfill the expected performance during the ceremony, but to our knowledge they have not documented their work or reflections in a publicly available form. The OSCE report points to the vague definition of their tasks and argue that "the IEC met rarely and its role appeared largely formalistic. Most IEC members with whom the OSCE/ODIHR EAM [4] met were not conversant with the system and relied entirely on the MLGRD[5]'s guidance and advice. This called into question the IEC's competence and its effectiveness as an oversight body." [22, p. 8]. It is noteworthy that this criticism stays within a technical framing of the event and the system of takings-for-granted within the IT community, which only a few members of the IEC share. However, the OSCE report does not mention the possibility of discussing the ceremony more explicitly in social and political terms, and thereby providing the politicians and the public with other kinds of arguments.

As mentioned in Section II, the term economy of truth emphasises that "Knowledge is the result of the community's evaluations and actions, and it is entrenched through the integration of claims about the world into the community's institutionalized behaviour. Since the acts of knowledge-making and knowledge protecting capture so much of communal life, communities may be effectively described through their economies of truth." [26, p. 6]. The above suggests that for the Norwegian trial, technologists did not include discussions about the witnessing and its quality in their economy of truth. They also did not consider other public aspects of the event, e.g. in what respect is the aforementioned replacement useful, desirable or promising. But then we beg the question why the organizers bothered to organize the Decryption and Counting Ceremony in the observed form and to make it public, if only computer scientists and other experts are considered reliable observers if not to speak of reliable witnesses? We feel strongly that it is prudent to start considering witnessing and observing as part of the economy of truth for any internet voting platform and respective ceremonies, in particular.

In broader terms, if we compare the ceremony to the democratic paper-based election in Norway, there are noteworthy differences in the kind of public that the various processes allow for. In Norway as well as in many other countries, the paper-based enactment does not only give the public the opportunity to observe the election, as the organizers of the Decryption and Counting Ceremony mention, but they are allowed to participate in the counting as volunteer election officials. If we take the distributed nature of the counting

[4]Election Assessment Mission.

[5]Ministry of Local Government and Regional Development.

process across numerous municipalities into account as well, it demonstrates the involvement of any voter who cares to participate, as well as it presumes that voters are able to count and understand the event. This means that they are accountable witnesses in the particular part of the event they take responsibility for, and it signifies a shared responsibility in terms of trusting/distrusting the counting of one's fellow citizens as the results are finally brought together in the Ministry.

The Decryption and Counting Ceremony, on the other hand, involves only computer scientists as reliable witnesses in the legitimate audience. However, there were also others in the audience, e.g. peers from the e-voting community, observers from various organizations, or representatives from other governments who want to know about the technology, and vendors. At the same time, anyone from anywhere in the world is, in principle, invited to take part via the online broadcasting. This position is strikingly different from the involvement in the local paper-based election process. The role of the audience may be described as attestive spectators[6] as opposed to active participants. Attestive spectators hardly qualify as witnesses in the way Shapin understands it, as they are not explicitly involved and accountable for the ceremony and the performance they attest to. In this respect, the verifier team is the only community that qualifies as a reliable witness. To what extent it is possible as well as acknowledged that spectators of different professional trainings may contribute to a debate is not clear. This is not so much meant as a criticism, but also as a way of exploring possible ways of making the event legible in broader terms. We believe that ordinary citizens may hardly choose to watch the online performance for entertainment, or even as a citizen duty, but perhaps engaged teachers might want to use the broadcasting in discussing democracy and technology for educational purposes. We do not know to what extent the event has had an impact for instance on politicians and their decision making, but obviously one can argue that the ceremony and the way it was presented makes it difficult for people outside of the community engaged in internet election to make sense of the performance.

J. Barrat i Esteve et al. raised the following concerns: "Internet voting was in its infancy when the Council of Europe Recommendations were written. We know now that e-enabled elections are far more complex than previously thought, not only technically, but also legally and from the procedural point of view. Yet, the recommendations say little on the legal basis, trying, on the contrary, to cover every possible situation in a technically neutral way" [3, p. 8]. The idea that internet voting can be understood in a technically neutral way, which we see as another way of putting that it is exclusively about counting and not accounting, as if counting votes efficiently without taking the dimensions and the quality of the witnessing into account was possible, brings with it major political consequences. One of them is that when Election Observation Bodies approve of election results, for instance on the basis of the Council of Europe's Recommendation on legal, operational and technical standards for e-voting, or on the basis of the Decryption and Counting Ceremony, they implicitly also approve of the radical changes in the way witnessing takes place, but without addressing this explicitly.

[6]We owe this expression to Ingvar Tjøstheim, personal communication.

As it is well known by now, the Norwegian government decided to stop the internet trials [18], based on the arguments that the parliament disagreed on the subject, and this subject was considered too important to allow for disagreement. Besides this, they stressed that ordinary voters do not understand the mechanisms involved in internet voting [18]. This is, of course, a perfectly legitimate way of expressing a political standpoint. We do not know whether the experiences of the politicians involved in the ceremony have had a say in this argument, but common experience as well as analyses such as the OSCE report [22] certainly support the idea that ordinary citizens do not usually understand this voting mode. These arguments are indeed important from a democratic point of view. But in addition, we would like to argue that an analysis of the economy of truth that takes the new conditions of witnessing into account would provide critics, as in this case the government, with additional arguments. These arguments would in turn point to some of the conditions internet voting depends on, by opening the back-box of how the counting, and hence the accounting, take place. It would eventually make the radical changes in the way democracy is understood more obvious in terms of public involvement. The point we want to make, based on the guidelines that Shapin's idea of trust and the economy of truth provide, is that it is possible to explore political and social aspects in the process as well as sketch what the IT community is doing, and what ordinary people arguably do not understand. The argument does not so much point to missing competences among the voters, but informs about the process and the kind of public involved in the internet voting experiment. Seeing is not necessarily believing, trust and distrust go hand in hand according to Shapin, and we may reject the idea of trusting people and arrangements, if we do not know how to relate to them. The argument also suggests proponents of internet voting to be explicit about the vision of democracy that they carry with them in terms of witnessing, among other things. Currently it seems that the idea of proxy is well accepted in the community of observers, as a logical consequence of the competences and complexities involved in internet elections and deciding about the efficiency in counting votes, but less discussed within a political context: Is this what people and their representatives in Norway or elsewhere want?

VI. Concluding Remarks

The Ministry of Local Government and Regional Development of Norway organized on election day a Decryption and Counting Ceremony in the internet voting trials of 2011 and 2013. Starting from the organizers' declared perception of the ceremony in 2013, as an effort to sustain trust in internet voting, we have introduced a pragmatic approach to trust, that underlines the inseparability of truth from the witnessing of how it is brought about. We have suggested that academic or political communities can also shape the economy of truth, including their systems of takings-for-granted in how they view the world. Based on this approach as well as a description of how the event is organized in terms of an overseeing body, the IEC, and a group of appointed verifiers, this paper has examined how the organizers made the event observable to the audience and emphasised the complexities in decrypting and counting votes as well as the specific framing of the event by the IT community.

We have also discussed the limits in trying to make sense

of the event exclusively from a technical counting perspective, and explored a broader understanding of truth-making and trust-making by including a discussion of the witnessing process and the idea of making it public. We have suggested that exploring a pragmatic approach to truth and trust may be helpful in the e-governance community, as well as in other communities engaged in the idea of trust in technology. More specifically, we believe that any government considering to adopt internet voting may benefit from taking on the job of articulating social and political perspectives on internet voting. This will bring two advantages. First, it will help with refining the requirements of the internet voting architecture, by creating a space for discussing how to improve the technical performance, by mechanisms other than zero-knowledge proofs, for example advanced logging infrastructures, time stamping, distribution, redundancy, and risk-limiting audits. Second, and just as importantly, it should articulate explicitly how witnessing is brought about, to what extent a public can take shape and how those processes transform the basis for representative democracy.

ACKNOWLEDGMENT

The authors were supported in part by the DemTech grant 10-092309 from the Danish Council for Strategic Research, Program Commission on Strategic Growth Technologies. The authors would also like to thank the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

[1] R.M. Alvarez, T.E. Hall, A.H. Trechsel. *Internet Voting in Comparative Perspective: The Case of Estonia*. Political Science and Politics, 42, pp. 497–505, 2009.

[2] J. Barrat i Esteve, B. Goldsmith, N. Turner. *International Experience with e-voting: Norwegian E-Vote Project*. IFES, June 2012.

[3] J. Barrat i Esteve, B. Goldsmith. *Compliance with International Standards: Norwegian E-Vote Project*. Washington, DC: IFES, 2012.

[4] C. Barry, I. Brightwell, L. Franklin. *iVote, Technology Assisted Voting*. Electoral Commission of New South Wales, November 2013.

[5] P.V.D. Besselaar, A. Oostveen, F.D. Cindio, D. Ferrazzi. *Experiments with E-Voting Technology: Experiences and Lessons*. Building the Knowledge Economy: Issues, Applications, Case Studies, IOS Press, 2003.

[6] C. Bull. *Safety first! Verifiability in the Norwegian e-voting System*. Seminar on Internet Voting, Norway, September 8, 2013.

[7] Expert Study Mission Report, *Internet Voting Pilot: Norway's 2013 Parliamentary Elections*. The Carter Center, March 19, 2014.

[8] The Electoral Knowledge Network. *Elections and Technology, Guiding principles*. aceproject.org/main/english/et/et20.htm (accessed 4 August 2014)

[9] T. ElGamal. *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Trans. on Inf. Th., 31 (4), pp. 469–472, 1985.

[10] Estonian Internet Voting Committee, videos (in Estonian). www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ/videos (accessed 4 August 2014)

[11] K. Gjøsteen. *The Norwegian Internet Voting Protocol*. IACR Cryptology ePrint Archive 2013, 473.

[12] J.A. Halderman, H. Hursti, J. Kitcat, M. MacAlpine, T. Finkenauer, D. Springall. *Security Analysis of the Estonian Internet Voting System*. Technical report, May 2014. estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf (accessed 4 August 2014)

[13] W. James. *Pragmatism*. Buffalo, N.Y., Prometheus Books, pp. 88–91, (1907) 1991.

[14] Kommunal og Regionaldepartamentet. *Regulations Relating to Trial Internet Voting During Advance Voting and Use of Electronic Electoral Rolls at Polling Stations on Election Day During the 2013 Parliamentary Election in Selected Municipalities*. June 19, 2013.

[15] D. MacKenzie. *Mechanizing Proof: Computing, Risk, and Trust*, MIT Press, 2001.

[16] Ministry of Local Government and Regional Development. *Internettvalstyret er oppnemnd*. Press release. June 20, 2013. (in Norwegian) www.regjeringen.no/en/archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/Nyheter-og-pressemeldinger/pressemeldinger/2013/internettvalstyret-er-oppnemnd-.html?id=731211 (accessed 26 May 2014)

[17] Ministry of Local Government and Regional Development. *Decryption and counting ceremony of the Internet votes, video.* (English language). www.regjeringen.no/en/dep/krd/Whats-new/news/2013/dekryptering--og-opptelling-av-internett.html?id=735379 (accessed 26 May 2014).

[18] Ministry of Local Government and Regional Development. *Ikke flere forsøk med stemmegivning over Internett*. Press release. June 23, 2014. (in Norwegian) www.regjeringen.no/nb/dep/kmd/pressesenter/pressemeldinger/2014/Ikke-flere-forsok-med-stemmegivning-over-Internett-.html?id=764300 (accessed 4 August 2014)

[19] News about the Norwegian e-voting trial in 2011 (in Norwegian). www.regjeringen.no/nb/dep/kmd/prosjekter/e-valg-2011-prosjektet/nyttomevalg/nytt-om-e-valg/2011.html?id=631622 (accessed 27 May 2014).

[20] OECD's Better Life Index. oecdbetterlifeindex.org/countries/norway (accessed 31 July 2014)

[21] OSCE/ODIHR, *Estonia: Parliamentary Elections 6 March 2011*. Election Assessment Mission Report. May 16, 2011.

[22] OSCE/ODIHR, *Norway: Parliamentary Elections 9 September 2013*. Election Assessment Mission Final Report. December 16, 2013.

[23] S.B. Segaard, H. Baldersheim, J. Saglie. *E-valg i et demokratisk perspektiv* Rapport (2012:005) Institutt for samfunnsforskning, Oslo, 2012.

[24] S.B. Segaard, D.A. Christensen, B. Folkestad, J. Saglie. *Internettvalg, hva gjør og mener velgerne?*, Rapport 2014:07, Institutt for samfunnforskning, Oslo, 2014.

[25] A. Shamir. *How to share a secret*. Communications of ACM 22, November 11, pp. 612–613, 1979.

[26] S. Shapin. *The Social History of Truth. Civility and Science in Seventeenth-Century England*. The University of Chicago Press, USA, 1994.

[27] J. Simon. *Trust*. Oxford Bibliographies in Philosophy, Oxford University Press, New York, 2013. www.oxfordbibliographies.com/view/document/obo-9780195396577/obo-9780195396577-0157.xml (accessed 4 August 2014)

[28] O. Spycher, M. Volkamer, R. Koenig. *Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting*. VoteID'11, Tallin, Estonia, 2011.

[29] I.G. Stenerud, C. Bull. *When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting*. Proceedings of EVOTE2012, LNI GI Series, Bonn.

[30] A.L. Strauss. *Continual Permutations of Action*. New York, Aldine de Gruyter, 1993.

[31] M. Volkamer, O. Spycher, E. Dubuis. *Measures to Establish Trust in Internet Voting*. ICEGOV'11, Tallin, Estonia, 2011.

[32] K. Vollan. *Final Verification Report from the Voting Card Printing and the Secure Handling of Cryptographic Keys*, Version 0.1 DRAFT. The Internet Voting Board Representative: Internet Voting Trial 2013, August 26, 2013.

[33] M. E. Warren. *Democracy and Trust*, Cambridge University Press, 1999.

Auditing and Verifiability

Proving the Monotonicity Criterion for a Plurality Vote-Counting Program as a Step Towards Verified Vote-Counting

Rajeev Goré
The Australian National University

Thomas Meumann
The Australian National University

***Abstract*—We show how modern interactive verification tools can be used to prove complex properties of vote-counting software. Specifically, we give an ML implementation of a vote-counting program for plurality voting; we give an encoding of this program into the higher-order logic of the HOL4 theorem prover; we give an encoding of the monotonicity property in the same higher-order logic; we then show how we proved that the encoding of the program satisfies the encoding of the monotonicity property using the interactive theorem prover HOL4. As an aside, we also show how to prove the correctness of the vote-counting program. We then discuss the robustness of our approach.**

I. Introduction

Paper-based elections consist of three main phases: printing and transporting ballot papers to polling places; collecting and transporting ballots after polling; and hand-counting ballots centrally to determine the result. Our confidence in the result is based on blind trust and scrutiny. We trust electoral officials to act honestly, but allow scrutiny by observers from political parties and independent organisations when ballots are transported, opened, and counted. That is, we rely on the difficulty of compromising all of these different non-centralised entities simultaneously. Such elections are slow to announce results, are (becoming) prohibitively expensive and impinge on the privacy of impaired voters who must be assisted by others to cast their vote. Paper ballots and hand-counting are therefore being replaced, gradually, by electronic alternatives [1], and although such vote-casting and vote-counting are very different aspects, they are often conflated into the term electronic voting.

End-to-end voter-verifiable systems attempt to provide full confidence by verifying the processed output of each phase rather than actually verifying any computer code. Such systems allow voters to verify that: their votes are cast correctly into a digital ballot; that these digital ballots are transported from the polling place to the central vote-counting authority without tampering; and that their digital ballot appears in the final tally. The methods used to guarantee these properties invariably involve sophisticated cryptographic methods, including methods for computing the sum of the encrypted votes without having to decrypt the votes themselves. But such cryptographic methods only work when the tallying process is a simple sum. No currently implemented "end to end voter-verifiable" system [2]–[5], can guarantee that votes are counted correctly using a complex preferential vote-counting method such as single transferable voting (STV). Thus there is no simple way to verify the output of the process of vote-counting using STV.

The accepted wisdom for elections that involve complex preferential vote-counting methods, such as STV, is to publish the ballots on a web page so that they can be tallied by multiple different implementations, built by interested (political) parties. That is, in e-voting, it is not the code that we should verify, but the processed output. For example. the Australian Electoral Commission (AEC) uses a computer program to count votes cast in senate elections. The program has been "certified" by a commercial certification company after conducting some testing, but has not been verified in any formal sense. The AEC makes the votes public but has refused to make the code public. Antony Green, a journalist and electoral commentator, has built his own implementation of the STV method used to count the votes. The only known "scrutiny" of the results of the previous senate election is the fact that Green's code produced the same results as those produced by the AEC computer code.

But what if the official results from the AEC differ from those of Green, or from those of the political party that loses? In particular, what if the losing party appeals to the court of disputed returns? There is no reason why the results of the AEC should be accepted over those of others. Do we resort to time-consuming and error-prone hand-counting to resolve the discrepancy? Or do we commission someone to write yet another program? Or do we enter a complex court case to argue the pros and cons of the two implementations? None of these options will engender confidence in the result, let alone e-voting itself. But if the AEC used a computer program that had been formally verified as correct, there would be a strong case to reject the conflicting results from other computer programs.

Thus, given the complexity of preferential vote-counting methods like STV, even the most secure and most sophisticated end-to-end voter-verifiable system will still fail to gain the trust of voters if it cannot guarantee that votes are not only cast correctly and transported without tampering but that they are also counted correctly.

Here, we focus on verified vote-counting where "verification" is the process of proving that an actual computer program correctly implements a formal specification of some desirable property. We first explain the various forms of software verification that are possible today and briefly explain the pros and cons of these approaches. We then describe our work on verifying that a computer program for counting votes according to a simple plurality voting scheme meets Arrow's monotonicity criterion. We also prove that the program counts votes correctly, which in this case, turns out to be relatively

simple. The case study nicely highlights the issues involved in formal verification of software.

How does our work tie into the electoral process and how does it help to improve it?

Most preferential vote-counting methods are simplified to make it possible to count the ballots by hand since humans are notoriously bad at such mechanical tasks. The greatest simplifications are usually made to the way ballots are transferred from one candidate to another even though the simplifications are known to engender some unfairness in the final tally. Simplifications are also made in tracing back through the previous rounds when breaking ties, again even though quite simple examples can be constructed which show that these approximations can lead to unfairness. Sometimes, the result can come down to a simple coin toss at some crucial juncture.

The ability to count votes using computers opens up the possibility to design new, even more complex, voting schemes which guarantee various theoretical desiderata, and to use them in real elections. How can we be sure that the new schemes enjoy the desired properties while remaining practical for counting by computer for large numbers of votes? More importantly, how can we convince voters that the safety-net provided by hand-counting is no longer necessary?

One way is to develop the voting scheme incrementally and iteratively. By starting with a simple implementation and a specification of a desired property, such as a fairness, and gradually adding complexity, we can iron out errors in the implementation and specification, and gain insights into the practicality of the desired theoretical desiderata. By involving electoral officials in this iterative process, we can ensure that they are convinced that the implementations meets the desired criteria beyond any doubt. Correctness is just one such criteria.

Our work has the potential to revolutionise elections using preferential methods of voting since it allows us to produce fairer, but necessarily complex, versions of vote-counting and produce computer programs that are guaranteed to implement these complex vote-counting methods correctly.

II. Various forms of Software Verification

Modern software verification methods can be broadly classified into two main categories which we shall call "light-weight" and "heavy-weight" for want of better terms.

Light-weight methods range from the fully automatic methods like software bounded model checking (SBMC) to full functional software verification using automatic annotation-based program verification tools such as VCC [6]. Both SBMC and annotation-based program verification tools involve adding the properties to be checked as pre and post condition annotations to the actual code, turning these annotations automatically into proof obligations by a compiler, and discharging the proof obligations automatically by some theorem prover. Their main advantage is that the proof-obligations are discharged fully automatically. Thus the user may have to learn some basics of how to annotate programs with pre- and post-conditions, and how to operate the verification tool, but the user does not have to be an expert in logic and formal proof. Their biggest disadvantage is that there is usually little that can be done when the verification tool fails to discharge the required proof obligations automatically. Even when the proof obligations are discharged automatically, there is no guarantee that the tool itself is sound or complete, lowering the trust that can be placed in the correctness of the program.

Heavy-weight verification involves encoding both the implementation and the specification into the logic of some theorem prover, and then proving that the encoding of the implementation implies the encoding of the specification using that theorem prover, usually interactively. The biggest advantage of this method is that we can trust the final proof completely. The disadvantage is that the user has to be expert in logic and formal proof.

III. Heavy-weight Verification Using HOL4

The verification process explored here falls under the rubric of heavy-weight verification. It involves producing a logical formalisation of both the program's requirements and the program itself in the HOL4 theorem proving assistant, then constructing a formal proof showing that the program matches the requirements. Why should we trust the HOL4 theorem proving assistant?

HOL4 is an (interactive) theorem prover based upon Dana Scott's "Logic for Computable Functions" (LCF), a mathematically rigorous logic engine consisting of 8 primitive inference rules which have been proven to be mathematically correct [7]. HOL4 implements this logic engine using approximately 3000 lines of ML code. This code has been scrutinised by experts in LCF to ensure that it correctly implements the 8 inference rules. Any complex inference rules must be constructed from the core primitive rules only. This means that proofs produced in HOL4 are highly trustworthy.

A side-effect of using an LCF-style proof assistant is that the program must be represented in higher-order logic. It thus becomes possible to prove various results about the program. This can be used to verify the voting scheme itself with respect to various desiderata. For example it would be possible to prove that the voting scheme in question adheres to the independence of irrelevant alternatives (see [8]). It is also possible to prove comparative results between different voting schemes: for instance that voting scheme A differs from voting scheme B in only x specific situations. The ability to reason about the program in this manner is what makes this process suited to the design of fairer voting schemes which can be rigorously tested against any desired properties.

IV. Case Study

As a case study, we implement a program for plurality vote-counting, verify that it obeys the monotonicity criterion, and also prove that it counts votes correctly.

A. Plurality Voting

First-past-the-post plurality voting is a voting scheme wherein each voter may vote for one candidate only, usually by marking a cross or a tick next to the desired candidate on the ballot paper. The number of votes for each candidate is tallied, and the candidate with the most votes (a relative majority) is declared elected. Note that the candidate does not need an absolute majority. Real-world voting systems vary in the way

they deal with a tie, but in our simple case, no candidate is elected in the case of a tie.

B. The Monotonicity Criterion (MC)

The monotonicity criterion was originally posited by Arrow as a property of social welfare functions as follows [8]:

> "If an alternative social state x rises or does not fall in the ordering of each individual without any other change in those orderings and if x was preferred to another alternative y before the change in individual orderings, then x is still preferred to y."

A social choice procedure, such as a voting scheme or a market mechanism, can be said to either satisfy this condition or not. Reducing the available social choice procedures to preferential voting schemes or a subset thereof allows us to narrow the definition and put it in more tractable language. Thus for our purpose: "social state" is the election of a particular candidate; and "x is preferred to y" refers to a societal preference and can be changed to "x is elected".

In our plurality system, voters may only vote for one candidate, ie. rank one candidate above all others (rejecting all others equally). Thus monotonicity can be rewritten as:

> If each voter either changes his or her vote to a vote for candidate x or maintains his or her vote unchanged, and x won before any votes changed, then x will still win after the changes.

C. Verification

The verification method involves producing a logical formalisation of both the program's requirements (the vote-counting legislation) and the program itself, then constructing a formal proof showing that the software matches the specification, using HOL4.

In other words, the proof procedure involves producing the following, step-by-step:

1) Implementation: An implementation in SML of the plurality vote-counting scheme.
2) Translation: A translation of the implementation into HOL4's formal logic.
3) Specification: An encoding of MC in HOL4's logic.
4) Proof: A proof acceptable to the HOL4 theorem prover that the specification (3) holds of the translation (2).

Each of these steps is explored individually below.

1) Implementation: A plurality vote-counting program has been written in StandardML (SML), a strict functional programming language. The SML code for the plurality counting program is given in Figure 1.

This implementation makes use of the `option` type operator. Specifically, `ELECT` returns a value of type `num option`. `WINNER` also makes use of the `num option` datatype. The `option` type operator is acting in both cases as a wrapper around type `num` to allow the program to return either a number (as `SOME` c) or the lack thereof (`NONE`). The statement `SOME` c is *not* shorthand for "there exists some c".

For simplicity, each candidate is represented by a number from 0 to $(C-1)$, and the set of votes by a list of numbers: each representing a vote for the numbered candidate. Let c_i be the i^{th} candidate and v_j be the j^{th} vote. A vote v_j is a vote for c_i iff the j^{th} member of the list `v` is equal to i. If $v_j < 0$ or $v_j \geq n$ where n is the number of candidates, then v_j is invalid.

Our implementation runs in $O(cv)$ time with number of candidates c and number of votes v. A $O(c+v)$ implementation is possible, but it was kept this way in order to maintain the program's functional purity and simplicity (thereby making it easier to reason about). Theoretically, the same results are provable of a $O(c+v)$ implementation but this is not explored here.

2) Translation into HOL4: Figure 1 shows the implementation translated into recursive definitions in HOL4. The translation between SML and HOL4 was done by hand, but was a purely mechanical process. Bar a few small syntactic differences, the translation clearly syntactically matches the SML implementation. Whether the HOL4 translation matches the SML implementation semantically is somewhat less clear. This issue is explored in more detail in section VI.

Note that the translation is a statement in higher order logic, not a program in the traditional sense. This is why the HOL4 function definitions consist of conjunctions (`/\` is the HOL4 syntax for logical 'and').

3) Specification: Formally stated in higher-order logic, the definition of monotonicity given on page 3 becomes:

$$\begin{aligned}
&\forall C\, w\, v\, v'.\ \Big((\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v) \\
&\wedge\ \big(\forall n.\, n < \texttt{LENGTH}\, v \Rightarrow (\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v')\big) \\
&\qquad\qquad \wedge\ (\texttt{ELECT}\, C\, v = \texttt{SOME}\, w)\Big) \\
&\qquad\qquad\qquad\qquad \Rightarrow (\texttt{ELECT}\, C\, v' = \texttt{SOME}\, w) \quad (1)
\end{aligned}$$

where:

- v is a list representing the set of initial votes;
- v' is a list representing the set of changed votes;
- w is a number representing the winning candidate;
- C represents the number of candidates;
- `LENGTH` l is the length of list l; and
- `EL` n l is the n^{th} element of list l, where $0 \leq n <$ `LENGTH` l.

Note that `LENGTH` and `EL` are predefined recursive functions in HOL4 and `EL` $0\ (h :: t) = h$. That is, the members of the list are numbered from 0, not 1.

The first conjunct in the antecedents of the implication (the first line) states that the number of votes cannot change. The second conjunct (second line) states that each vote in the set of changed votes must be a vote for the winner, or the same as the corresponding initial vote, or both. The third conjunct (third line) states that there is a winner from the set of initial votes. The final line states that these conjuncts together imply that the winner still wins with the changed votes.

```
local
  (* Counts the number of votes in the
     given list for candidate c. *)
  fun COUNTVOTES c []     = 0
    | COUNTVOTES c (h::t) = if h = c
                        then 1 + COUNTVOTES c t
                        else 0 + COUNTVOTES c t;

  (* Finds winner from all candidates
     numbered c or lower. *)
  fun WINNER 0 v = (SOME 0, COUNTVOTES 0 v)
    | WINNER c v =
      let
        val numvotes = COUNTVOTES c v
      in
        let
          val (w, max) = WINNER (c-1) v
        in
          if numvotes > max
            then (SOME c, numvotes)
          else if numvotes = max
            then (NONE, max)
          else (w, max)
        end
      end;
in
  (* C is the number of candidates, v is the
     list of votes *)
  fun ELECT C v = if C <= 0 then NONE
                  else #1 (WINNER (C-1) v)
end;
```

(a) SML

```
val COUNTVOTES_def = Define `
  (COUNTVOTES c []     = 0) /\
  (COUNTVOTES c (h::t) = if (h = c)
                    then 1 + COUNTVOTES c t
                    else 0 + COUNTVOTES c t)`;

val WINNER_def = Define `
  (WINNER 0 v = (SOME 0, COUNTVOTES 0 v)) /\
  (WINNER c v =
    let
      numvotes = COUNTVOTES c v
    in
      let
        (w, max) = WINNER (c-1) v
      in
        if numvotes > max
          then (SOME c, numvotes)
        else if numvotes = max
          then (NONE, max)
        else (w, max))`;

val ELECT_def = Define `
  ELECT C v = if C <= 0 then NONE
              else FST (WINNER (C-1) v)`;
```

(b) HOL4

Fig. 1: Implementation of a plurality counting algorithm (a) in SML, and (b) translated into HOL4.

4) Proof: The entire proof was completed using the HOL4 theorem prover. Rather than explaining the syntax of HOL4 and how it corresponds to higher-order logic, all of the formulae in this section are given using standard higher-order logic syntax.

Let ϕ be defined as follows:

$$\phi = \Big(\big(\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v\big) \wedge \big(\forall n.\, n < \texttt{LENGTH}\, v \Rightarrow (\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v')\big)\Big) \tag{2}$$

This allows us to rewrite the proof obligation (1) as:

$$\forall C\, w\, v\, v'.\, \big(\phi \wedge (\texttt{ELECT}\, C\, v = \texttt{SOME}\, w)\big) \Rightarrow (\texttt{ELECT}\, C\, v' = \texttt{SOME}\, w) \tag{3}$$

C is either 0 or the successor to some number (ie. $\texttt{SUC}\, x$). Examining these cases and applying some basic substitution allows us to rewrite the proof obligation (3) in terms of WINNER:

$$\forall c\, w\, v\, v'.\, \big(\phi \wedge (\texttt{FST}\, (\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w)\big) \Rightarrow (\texttt{FST}\, (\texttt{WINNER}\, c\, v') = \texttt{SOME}\, w) \tag{4}$$

The new proof obligation is that at any stage of the recursion: if w beats all other candidates examined so far with the initial votes, then w beats the same candidates with the changed votes.

To get to the core of the problem, it is desirable to go one step further and rewrite the proof obligation in terms of COUNTVOTES. In order to do this, we need a formula relating WINNER and COUNTVOTES. The following lemma states that if w beats all candidates numbered c or less, then w also has more votes than all of the said candidates and vice versa. The proof of this lemma relies upon inductive proofs of various properties of WINNER:

$$\forall c\, v\, w.\, w \leq c \Rightarrow \big((\texttt{FST}\, (\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w) \iff \forall c'.\, c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v\big) \tag{5}$$

The proof obligation (4) can thus be rewritten in terms of COUNTVOTES as follows:

$$\forall c\, w\, v\, v'.\, \big(\phi \wedge (\forall c'.\, c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v)\big) \Rightarrow (\forall c'.\, c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v' > \texttt{COUNTVOTES}\, c'\, v') \tag{6}$$

In other words we need to prove that if w has more votes than the set of lesser-numbered candidates using the initial votes, and the conditions in ϕ hold, then w also has more votes than all the aforementioned candidates using the changed votes. A structural case analysis of v and v' can now be performed (the lists being either empty or having a head and tail).

In order to make the proof fall all the way through it is necessary to prove the following properties of `COUNTVOTES`:

$$\forall w\, v\, v'.\ \phi \Rightarrow \texttt{COUNTVOTES}\ w\ v' \geq \texttt{COUNTVOTES}\ w\ v \quad (7)$$

$$\forall w\, v\, v'.\ \phi \Rightarrow (\forall c.\ c \neq w \Rightarrow \texttt{COUNTVOTES}\ c\ v \geq \texttt{COUNTVOTES}\ c\ v') \quad (8)$$

Appendix A lists all the lemmas involved in the proof and a diagram of their inter-dependencies.

V. Correctness

The astute reader will have noticed that we have not proved the correctness of our encoding of our implementation by proving that the winner is the candidate with the most number of votes. The HOL4 formula to capture this correctness statement is:

$$\forall C\, v\, w.\ w < C \Rightarrow (\texttt{ELECT}\ C\ v = w \iff \forall c'.c' \neq w \wedge c' < C \Rightarrow \texttt{COUNTVOTES}\ w > \texttt{COUNTVOTES}\ c') \quad (9)$$

Given the lemmas proved during the proof process for the monotonicity criterion, this is a quick and easy process. It has been left out for brevity.

VI. Summary and Discussion

There are two aspects worth considering when evaluating the feasibility of our verification process: the effort involved and whether the proof actually covers everything that is required. We address each in turn.

We have proved that our recursive definitions in HOL4 match our encoding of MC. Syntactically, our SML program appears equivalent to our recursive definitions. Semantic equivalence is another matter. We have no formal guarantee that our SML implementation is equivalent to our HOL4 translation, except for their syntactic similarity.

A particularly illuminating example of this conundrum is the difference between HOL4's and SML's handling of numerical types. In both programs, the candidates are represented by numbers. SML uses integers by default, which can be positive or negative: `~1`, `0`, `1`, `2` etc. HOL4, on the other hand, uses Peano numbers, which can only be `0` or the successor to some number. That is, they can only be positive: `0`, `SUC 0`, `SUC (SUC 0)` etc. The underlying representation would not matter if the same operations were defined and those operations had the same effect. This is not the case, however. $0 - 1 = 0$ is provably correct in HOL4, whilst `0 - 1` will result in `~1` in SML (`~` is unary negation in SML so `~1` means -1). We are safe however, since our SML implementation deals only with positive integers.

One way to get around this is to execute the HOL4 definitions directly. After all, the encoding in HOL4 is itself executable using HOL4's deductive rewriting engine. Unfortunately there is a large loss in efficiency when using this method. The SML implementation takes less than 7 minutes, using less than 10.5 GiB of memory, to count 250 *million* votes with 160 candidates. By contrast, with the same number of candidates, the HOL4 translation takes 40 minutes, using 14 GiB of memory, to count 25 *thousand* votes. Also, since the logical statements must be built up using the primitive core rules of logic, it is impractical to convert a list of votes into a logical statement acceptable to HOL4.

Another way would be to write the HOL4 specification first, and automatically produce the SML implementation using a verified compiler. This is a non-trivial task. There is, in fact, a project underway aimed at automating this translation: CakeML (https://cakeml.org/) [9]. It is currently under development so is not explored here, but may in future provide the missing link required.

Currently, our confidence in the correctness of our SML program rests completely on the syntactic similarity between the SML code and its HOL4 encoding, and the assumption that syntactic similarity implies semantic equivalence. As explained above, this holds for the case study explored here. For more complex voting schemes, we envisage that an iterative process may be necessary to reduce the syntactic differences between the SML code and its encoding in HOL4 (under the assumption that syntactic similarity implies semantic equivalence). This may require extending the HOL4 theorem prover to include more complex constructs from SML which may be needed to efficiently implement more complex voting schemes.

The entire process from implementation to complete verification took 3 weeks. Bear in mind that this was a learning process, with only 1–2 months-worth of prior experience with HOL4. Ultimately, 3 weeks is a short time to spend producing a piece of fully formally verified software. How this scales to more complex problems remains to be seen.

Another measure of the effort involved is the proof-to-implementation ratio, measured in lines of code (LoC). The implemented algorithm spans 24 lines whilst the proof spans 590. This gives at least 24 lines of proof for each line of implementation. Unfortunately, the final LoC measurement does not take into account the effort expended in exploring unproductive proof strategies. This makes its applicability here questionable. Nevertheless, it may be helpful when comparing the procedure to other verification methods. Assuming the ratio can be extrapolated to larger programs, verifying a 100-line program would require 2400 lines of verification.

It is also worth noting that the methodology here is not well suited to rapid prototyping. In particular, an indeterminate amount of time can be spent attempting to prove an invalid property before realising it is impossible.

VII. Conclusion

Given the simplicity of the algorithm for plurality voting, it is questionable whether our formal proof of correctness is significant. Note, however, that the proof that our plurality voting algorithm obeys monotonicity is far from trivial. Thus our procedure for fully formally verifying complex properties of vote counting algorithms is clearly feasible for small simple

algorithms. It remains to be seen whether the procedure will scale to complex proportional representation systems.

The verification approach took roughly 10 weeks of full time work: 7 weeks of learning HOL4 and 3 weeks to specify and verify the code. Given the trustworthiness of the HOL4 proof assistant and the associated rigorousness of the proof, this seems a small price to pay. However, the following caveats apply. We verified a HOL-encoding of an SML program, not the SML program itself, so we have no proof of their equivalence. A visual comparison is compelling for the simple case we examined here, but might not be for a complex STV voting scheme used in real elections. The HOL4 encoding of plurality voting is itself executable, but is only feasible for small-scale elections. The CakeML project, currently under active development, may provide a solution that could be used to bridge this gap. Also, the interactive proof methodology does not lend itself to rapid prototyping since it does not provide counter-examples. Indeed, one can spend an inordinate amount of time trying to prove false conjectures before realising that they are indeed false.

VIII. Further Work

Our aim in the future is to extend this case study to formally verify the correctness of an SML implementation of Hare-Clark, a complex STV voting scheme used in a number of jurisdictions around the world, including Ireland, Australia and New Zealand.

Since submitting this paper, we have encoded the Hare-Clark Act which specifies the STV method used to count votes in the Australian state of Tasmania into approximately 800 lines of HOL. We have also written a matching program of approximately 200 lines of SML to count votes according to this method and have encoded the SML program into HOL. We were able to keep the syntactic similarity between the HOL encoding of the SML program and the SML program itself so we are confident that the HOL encoding captures the program correctly. Tests show that our SML program can easily count 0.5 million votes for 10 candidates in approximately 0.5 seconds. It remains to prove inside HOL4 that the HOL encoding of the SML program implies the HOL encoding of the Hare-Clark Act. We are therefore confident that the methodology outlined here will scale to allow us to formally verify complex real-world instances of STV as used in various jurisdictions around the world.

Acknowledgment

We thank Dr Jeremy Dawson for his guidance in the use of the HOL4 theorem prover.

References

[1] D. W. Jones and B. Simons, *BROKEN BALLOTS: Will Your Vote Count?* CSLI Publications, Stanford, USA, 2012.

[2] Pret-A-Voter, "Prêt à Voter," http://www.pretavoter.com/, Accessed January 28, 2013.

[3] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *IEEE Security and Privacy*, vol. 2, no. 1, pp. 38–47, 2004.

[4] Helios, "Helios," http://heliosvoting.org/.

[5] D. Chaum, A. Essex, R. T. C. III, J. Clark, S. Popoveniuc, A. T. Sherman, and P. Vora, "Scantegrity: End-to-end voter verifiable optical-scan voting," *IEEE Security & Privacy*, vol. 6, no. 3, pp. 40–46, 2008.

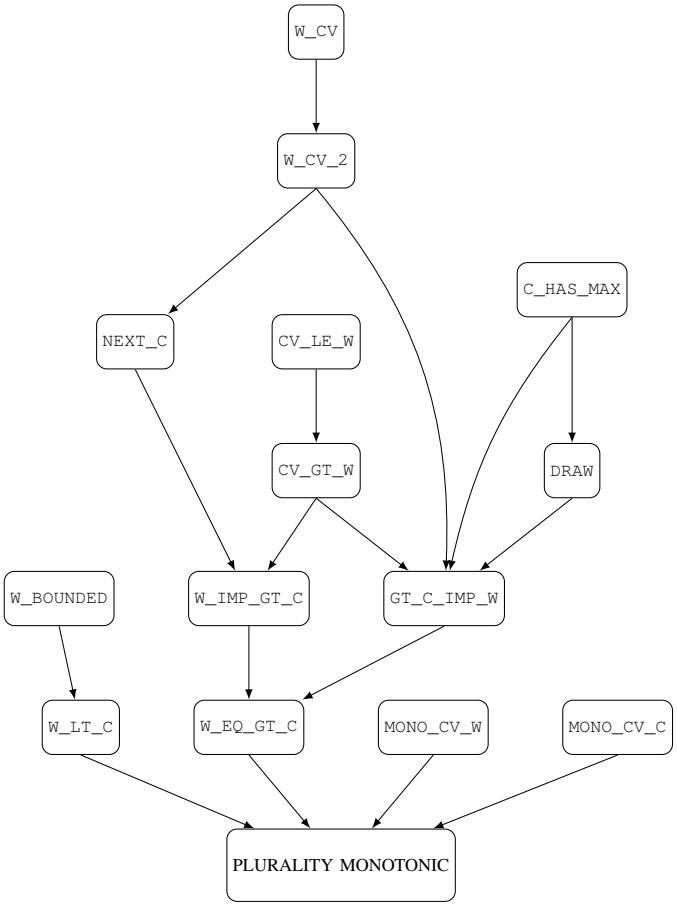


Fig. 2: Dependencies between lemmas. The proof of a lemma at the destination of an arrow relies upon the lemma at the arrow's origin.

[6] E. Cohen, M. Dahlweid, M. Hillebrand, D. Leinenbach, M. Moskal, T. Santen, W. Schulte, and S. Tobies, "VCC: A practical system for verifying concurrent C," in *Theorem Proving in Higher Order Logics*, ser. Lecture Notes in Computer Science, S. Berghofer, T. Nipkow, C. Urban, and M. Wenzel, Eds. Springer Berlin Heidelberg, 2009, vol. 5674, pp. 23–42. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03359-9_2

[7] M. J. C. Gordon and T. F. Melham, *Introduction to HOL: a theorem proving environment for higher order logic*. CUP, 1993.

[8] K. J. Arrow, "A difficulty in the concept of social welfare," *Journal of Political Economy*, vol. 58, no. 4, pp. pp. 328–346, 1950.

[9] R. Kumar, M. O. Myreen, M. Norrish, and S. Owens, "Cakeml: a verified implementation of ML," in *POPL*, 2014, pp. 179–192.

Appendix

The following is a full listing of each lemma proved during the HOL4 proof. Figure 2 shows the dependencies between the various lemmas. See Section IV-C4 for an explanation of the proof.

`CV_LE_W`:

$$\forall c\, v\, c'.\ c' \leq c \Rightarrow \texttt{COUNTVOTES}\ c'\ v \leq \texttt{SND}\ (\texttt{WINNER}\ c\ v) \quad (10)$$

CV_GT_W:

$$\forall v\, c\, c'.\ c' < \texttt{SUC}\, c \wedge \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v > \texttt{SND}\,(\texttt{WINNER}\, c\, v) \Rightarrow \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v > \texttt{COUNTVOTES}\, c'\, v \quad (11)$$

W_BOUNDED:

$$\forall c\, v\, c'.\ c' > c \Rightarrow (\texttt{FST}\,(\texttt{COUNTVOTES}\, c\, v) \neq \texttt{SOME}\, c) \quad (12)$$

W_CV:

$$\forall c\, v\, w\, m.\ (\texttt{WINNER}\, c\, v = (\texttt{SOME}\, w, m)) \Rightarrow (\texttt{COUNTVOTES}\, w\, v = m) \quad (13)$$

W_CV_2:

$$\forall c\, v\, w.\ (\texttt{SOME}\, w = \texttt{FST}\,(\texttt{WINNER}\, c\, v)) \Rightarrow (\texttt{COUNTVOTES}\, w\, v = \texttt{SND}\,(\texttt{WINNER}\, c\, v)) \quad (14)$$

NEXT_C:

$$\forall v\, w\, c.\ (\texttt{SOME}\, w = \texttt{FST}\,(\texttt{WINNER}\, c\, v)) \wedge \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v < \texttt{SND}\,(\texttt{WINNER}\, c\, v) \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v \quad (15)$$

W_IMP_GT_C:

$$\forall c\, v\, c'\, w.\ \big((c' \neq w) \wedge (c' \leq c) \wedge (\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w)\big) \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v \quad (16)$$

C_HAS_MAX:

$$\forall v\, c.\ \exists c'.\ c' \leq c \wedge (\texttt{COUNTVOTES}\, c'\, v = \texttt{SND}\,(\texttt{WINNER}\, c\, v)) \quad (17)$$

DRAW:

$$\forall v\, c.\ (\texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v = \texttt{SND}\,(\texttt{WINNER}\, c\, v)) \Rightarrow \exists c'.\ c' \leq c \wedge (\texttt{COUNTVOTES}\,(\texttt{SUC}\, c)\, v = \texttt{COUNTVOTES}\, c'\, v) \quad (18)$$

GT_C_IMP_W:

$$\forall c\, v\, w.\ w \leq c \Rightarrow \big((\forall c'.\ c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v) \Rightarrow (\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w)\big) \quad (19)$$

W_EQ_GT_C:

$$\forall c\, v\, w.\ w \leq c \Rightarrow \big((\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w) = (\forall c'.\ c' \neq w \wedge c' \leq c \Rightarrow \texttt{COUNTVOTES}\, w\, v > \texttt{COUNTVOTES}\, c'\, v)\big) \quad (20)$$

W_LT_C:

$$\forall c\, v\, w.\ (\texttt{FST}\,(\texttt{WINNER}\, c\, v) = \texttt{SOME}\, w) \Rightarrow w \leq c \quad (21)$$

MONO_CV_W:

$$\forall w\, v\, v'.\ (\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v) \wedge \big(\forall n.\ (n < \texttt{LENGTH}\, v) \Rightarrow ((\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v'))\big) \Rightarrow \texttt{COUNTVOTES}\, w\, v' \leq \texttt{COUNTVOTES}\, w\, v \quad (22)$$

MONO_CV_C:

$$\forall w\, v\, v'.\ (\texttt{LENGTH}\, v' = \texttt{LENGTH}\, v) \wedge \big(\forall n.\ (n < \texttt{LENGTH}\, v) \Rightarrow ((\texttt{EL}\, n\, v' = w) \vee (\texttt{EL}\, n\, v = \texttt{EL}\, n\, v'))\big) \Rightarrow \forall c.\ c \neq w \Rightarrow \texttt{COUNTVOTES}\, c\, v \geq \texttt{COUNTVOTES}\, c\, v' \quad (23)$$

Efficiently Auditing Multi-Level Elections

Joshua A. Kroll
Princeton University
Princeton, NJ 08544
kroll@cs.princeton.edu

J. Alex Halderman
University of Michigan
Ann Arbor, MI 48109
jhalderm@eecs.umich.edu

Edward W. Felten
Princeton University
Princeton, NJ 08544
felten@cs.princeton.edu

ABSTRACT

In a multi-level election, voters are divided into groups, an election is held within each group, and some deterministic procedure is used to combine the group results to determine the overall election result. Examples of multi-level elections include U.S. presidential elections and some parliamentary elections (such as those with regional groupings of voters). The results of such an election can hinge on a few votes in one group, while being insensitive to large shifts within other groups. These disparities create opportunities to focus election integrity efforts in the places where they have the highest leverage. We consider how to improve the efficiency of post-election audits, such as those that compare paper ballots to corresponding electronic records, in multi-level elections. We evaluate our proposed solutions using data from past elections.

I. Introduction

A *multi-level election* divides voters into disjoint groups, holds an election within each group, and then applies some deterministic procedure to combine the group results into an overall election result. In this paper, we discuss how to audit multi-level elections efficiently.

An important attribute of multi-level elections is that some ballots may have much more influence than others [1], [2], [3], [4]. For example, in the 2000 U.S. presidential election, a shift of 269 votes in the state of Florida would have changed the national election result, while a shift of 350,000 votes in Texas, or a shift of every vote in the most populous state, California, would not have changed the result. These non-uniformities create opportunities to focus election integrity efforts where they will do the most good. After an election, we can focus our post-election auditing resources to get the highest confidence in the overall election result, at the lowest total cost.

Post-election auditing can help to provide confidence in the integrity of an election by providing evidence that the votes were counted-as-cast. Several electronic election technologies generate redundant copies of ballot data, such as (now widely deployed) optical scan voting systems, in which voters mark paper ballots and scanned images of those ballots are tabulated electronically [5], or systems with a voter-verified paper audit trail, in which voters make a selection electronically and a copy of their selection is printed for review before being dropped automatically into a ballot box [6]. In any system with redundantly stored ballot data (e.g. electronically and on paper), we can audit by comparing the electronic record to the auxiliary record on a per-ballot basis. Generally, the electronic version of the ballot data will be much faster and cheaper to gather and tabulate and the auxiliary record will be much more costly to examine. Thus, we want to minimize the number of auxiliary records that must be examined, while also establishing high confidence that a full examination of all auxiliary records would yield the same election result as the reported electronic result. Efficient post-election auditing relies on examining a subset of the auxiliary records, comparing them to the corresponding electronic records, and relying on statistical arguments to confirm the election result to high statistical confidence.

Much prior work describes efficient approaches to ballot-based auditing in elections with simple majority or plurality rules for determining the election winner from votes cast [7], [8], [9], [10], [11], [12], [13], [14]; this work is the first to consider the case of multi-level elections and how the structure of the election's victory conditions can be used to reduce the total amount of auditing necessary to achieve a certain level of confidence.

Jones gives an overview of the need for and approaches to election auditing [15] and Dopp gives a more complete history of election auditing techniques [16].

Multi-level elections are common. One example is a U.S. presidential election, in which the voters are divided into 51 groups, one for each state.[1] Each state is assigned a certain number of electoral votes. Almost all of the states assign the state's electoral votes to the plurality winner of the state's election. (Two states, Maine and Nebraska, use a different procedure that can divide the state's electoral votes among candidates.) The states' results are combined by summing the electoral votes of each candidate. If one candidate receives a majority of electoral votes, that candidate is the winner. If no candidate receives a majority of electoral votes, then the election result is "undetermined" and the Congress holds a special vote to choose the President.

Another example is a national vote in certain parliamentary systems, where each district chooses a party representative, and representatives from the same party are assumed to act as a single coordinated bloc.[2] In such an election, the result is the identity of the party that holds a majority of seats; or lacking a single party with a majority, the result is the set of minimal coalitions, that is, a set of all of the minimal sets of parties that can form a coalition government. For example, if there are four parties, A, B, C, and D, which have 42, 29, 20, and 9 seats respectively for a total of 100 seats, then the minimal majority coalitions could be formed by parties A and B (71 seats); or by parties A and C (62 seats); or by parties A and D (51 seats); or by parties B, C, and D (58 seats).

Although the practical examples we discuss all determine the overall result by some kind of weighted counting of the individual group results, our theory is much broader than this and can handle any method for combining group results, including, for example, non-monotone systems in which winning more groups can make one's overall result worse. Our theory also extends naturally to handle elections with more than two levels.

The remainder of the paper is structured as follows. In Section II we discuss how to audit multi-level elections. In Section II-A, we work an example showing that considering an election's multi-level structure can reduce auditing costs. In Section II-B and for the rest of the paper, we develop the necessary theory to understand this phenomenon and use it to minimize overall auditing costs. We give an optimal auditing algorithm in Section II-C based on linear programming and in Section II-D, we give an approximation that is sometimes more efficient to compute. In Section II-E and Section II-F, we evaluate these methods using data from several recent elections. We finish by remarking on future work in Section III.

II. Auditing Multi-Level Elections

Post-election auditing is a statistical process for verifying, to some specified level of confidence, that the reported election result is consistent with the available evidence [15]. We assume that there is auxiliary evidence associated with each ballot which can be compared to the reported votes from that ballot, and that the auxiliary evidence is usually unexamined due to cost or time factors [8]. For example, in an optical-scan voting system, the reported results are determined by machine scanners in the polling place, and the auxiliary records are the paper ballots filled out by voters, which can be examined by hand and compared to the machine-reported results. A post-election audit will choose a sample of ballots and compare the chosen ballots with their auxiliary information. If the ballots in the sample are consistent with their auxiliary information, to within a specified tolerance, the audit succeeds; otherwise it fails and further investigation of the election is required.

The purpose of an audit is to reject by statistical means the hypothesis that a full examination of the auxiliary evidence would suggest a different overall election result than the one that was reported. This must be done to some specified level of statistical confidence (sometimes called

[1] For this purpose, the District of Columbia is treated as a state.

[2] This is not a requirement—party members may later defect on particular issues and vote with their opposition. However, we observe that when forming a government, it is especially common for parties to act as blocs (and this is generally expected), making such an assumption reasonable.

the "risk limit" [14]),[3] such as 99%. There is a rich literature on election auditing in one-level popular-vote elections (see [16], [17], [15], [7], [18], [19], [10], [9], [20], [21], [11]). Our method for multi-level auditing could be used with any method that satisfies some general assumptions, as we describe in Section II-C.

Our approach to multi-level auditing will be to assign an auditing responsibility to each group, and then argue that if all groups meet their responsibilities, the overall election result is confirmed in the necessary statistical sense. Because different groups may have a very different impact on the outcome in a multi-level election, we find that auditing to different levels of confidence in different groups can reduce significantly the cost of auditing the entire election to a specified overall level of statistical confidence, $1-\varepsilon$, as we can take advantage of choices about where to direct auditing resources.

Specifically, if the required confidence in the overall result is $1-\varepsilon$, then we will assign group i the responsibility to audit its result to a possibly different confidence level $1-\varepsilon_i$. We will assign the ε_i values such that audit success in every group implies that the overall election result is confirmed with the necessary confidence level.

If an audit in some group fails to confirm the election result, the audit will specify some escalation procedure that aims to determine the correct result in that group. If, ultimately, the election result is changed in some group, it will be necessary to re-evaluate the auditing responsibility assigned to all other groups to ensure that the required confidence level is met. This may necessitate re-auditing or the auditing of additional ballots in some locations if, for example, the auditing responsibility increases in group g' because auditing has changed the reported result in group g. The exact details of escalation will naturally depend on the nature and design of the overall election and the selection procedure that determines the overall result from the outcome in each group.

[3]We stress that, while prior work on election auditing has used the term "risk limit" to describe the acceptable bounds on confidence in the election result, we choose to call this parameter *statistical confidence*, as is done in many other fields. Nonetheless, the concepts are identical: both measure the bounds on the uncertainty in the correctness of the measured election result.

A. Election Auditing: An Illustrative Example

To illustrate the mechanics of multilevel election auditing, we will consider the case of presidential elections in the imaginary Republic of Freedonia. Freedonian voters are divided into five districts, District 1 through District 5. They vote directly for candidates for their country's highest office, President. In order to be elected President, a candidate must win a majority of the votes in at least three of the five districts. Thus, Freedonia has a multi-level election: first, candidates must win in each district and second, candidates must win across a majority of districts.

Citizens in Freedonia vote by marking a paper ballot which is scanned by an optical scanning machine that enables fully automated electronic tabulation of the paper ballots. Freedonian election officials wish to verify that the result reported by tabulation of the electronic records is consistent with the paper ballots. They will do this by a statistical procedure designed to verify consistency to 99% statistical confidence, that is, so that any discrepancy between the results will be detected with at least 99% probability. Their goal is to achieve this level of confidence at the lowest cost.

Consider now a specific election in Freedonia between two candidates for President, Alice and Bob. Table I summarizes the results of the election. How should this election be audited?

The most obvious way to audit this election is to conduct a separate audit in each district, to a confidence level of 99% within each district. Because the election within each district uses a simple majority criterion, we can use a standard auditing algorithm from the literature. Calandrino's method [8] would audit 233 ballots in District 1, and 25 ballots in each of Districts 2, 3, and 4, for a total of 308 ballots. (No audit is necessary in District 5 because District 5 did not contribute to Alice's reported victory.) The election result is be confirmed if, for every one of the audited ballots, manual reading of the ballot matches the electronic result reported for the same ballot.

In this case, it is not necessary to audit each individual district to 99% confidence. The reason for this is that Alice was reported as winning four districts when only three were required for victory, so that an incorrect result in only one district could not affect the outcome of the election. In

Candidate	District 1	District 2	District 3	District 4	District 5
Alice	51%	60%	60%	60%	35%
Bob	49%	40%	40%	40%	65%

TABLE I. RESULTS OF THE FREEDONIAN ELECTION, BY DISTRICT.

this case it is sufficient to audit to 90% confidence in Districts 1, 2, 3, and 4. To see why, suppose the election result is incorrect in two districts. If we audited the election 100 times, the audit would detect a discrepancy in the first district in 90 cases, and of the remaining ten cases, a discrepancy would be detected in the second district in nine cases. Only one case out of 100 would go undetected, which yields the required 99% detection rate. Following this procedure, we would audit 116 ballots in District 1 and 13 ballots in each of Districts 2, 3, and 4, for a total of 155 ballots.

Both of the audit strategies we have described so far spend the majority of auditing effort in District 1 (233/308 ballots in the first case, 116/155 ballots in the second case). In general, more ballots must be audited where the election result is close, because only a few miscounted ballots would be sufficient to swing the election and we need to audit more ballots to be confidence that we will randomly choose one of the few miscounted ones. By contrast, when the reported result is not close, auditing fewer ballots yields higher confidence.

This suggests a strategy in which we audit to lower confidence in District 1 and to relatively higher confidence in the other districts. The most extreme version of this strategy does no auditing at all in District 1, and audits to 99% confidence in Districts 2, 3, and 4. The logic of this approach is to establish with 99% confidence that Alice won all of Districts 2, 3, and 4, which is enough to establish that she won the election with 99% confidence, regardless of the accuracy of the reported District 1 results. In this approach we audit 25 ballots in each of Districts 2, 3, and 4, for a total of 75 ballots.

The Freedonia example shows that clever multilevel auditing strategies can reduce substantially the cost of auditing without reducing confidence in the result. It also illustrates some of the strategies that are possible. The results of analyzing this example are summarized in Table II.

The remainder of this paper presents a general mathematical theory for finding the lowest-cost strategy for auditing the result of any election conducted under a multi-level election procedure.

B. Basic Theory of Multi-Level Auditing

Intuitively, if the result of a multi-level election is incorrect, then it must be the case that the within-group result is incorrect for a sufficiently large set of the constituent groups. We define a *flipset* to be a set of groups such that changing the election results in all of these groups would have changed the overall election result. For example, in a U.S. presidential election, a flipset is a set of states which, if they all changed their results, would collectively change the total electoral college winner. We will say that F is a *minimal flipset* if F is a flipset but no proper (i.e., smaller) subset of F is a flipset. If F is a flipset, then there is some minimal flipset F^* such that $F^* \subseteq F$.

It is easy to show that if α_i are chosen so that for every minimal flipset F, $\sum_{i \in F} \alpha_i \geq 1$, and if the reported result in every group i is confirmed to confidence level $1 - \varepsilon^{\alpha_i}$, then the overall election result is confirmed to confidence level $1 - \varepsilon$. The intuition behind the proof is that if the reported overall election result is wrong, then there must be some minimal flipset F^* such that the reported group results are wrong for every group in F^*. The probability that the audits will fail to notice anything wrong anywhere in F^* is $\prod_{i \in F^*} \varepsilon^{\alpha_i} = \varepsilon^{\sum_{i \in F^*} \alpha_i}$ which by assumption is at most ε.

Cox gives a taxonomy of voting systems [22]. Our methods apply to any voting system which partitions voters into disjoint groups and holds an election in each group, subject to the constraint that the outcome at each level above the first is determined simply from the win or loss condition at the previous level (and not properties specific to the voting system used, such as vote counts).[4]

C. Optimal Auditing for Multi-Level Elections

We now turn to the question of how to minimize the cost of auditing a multi-level election.

[4] *Mixed member proportional* systems, such as the one used for parliamentary elections in Germany, do not have this property.

District	99% Confidence/District	90% Confidence/District	Optimal
District 1	233	116	0
District 2	25	13	25
District 3	25	13	25
District 4	25	13	25
Total	308	155	75

TABLE II. COST OF AUDITING THE FREEDONIAN ELECTION, IN TERMS OF NUMBER OF BALLOTS EXAMINED, BY STRATEGY EMPLOYED.

We allow the use of any known auditing scheme within each group. Our only assumption is that the expected cost C_i of auditing group i to confidence level $1-\varepsilon^{\alpha_i}$ can be expressed as $C_i = t_i \cdot \alpha_i$ for a group-specific coefficient t_i. Because t_i is the *expected* cost coefficient, our model can accommodate underlying audit methods that make adaptive decisions as to when to stop auditing, as well as schemes that have different audit costs for different ballots within a group.

We start by observing that many auditing schemes have a linear cost property, so that the expected cost of auditing a group of ballots to confidence level $1-\varepsilon^{\alpha_i}$ is proportional to α_i, with the constant of proportionality depending on the auditing scheme and the number and distribution of ballots. This constant will typically differ from group to group.

To see why linearity is a natural relation, consider that many auditing algorithms operate by performing a test (such as examining one ballot) and repeating the test, with an independent random selection, as many times as necessary until a desired confidence level is reached. If one test costs C_0 and achieves confidence $1-\varepsilon^{\alpha_0}$, then repeating the test k times (and failing if any of the k instances fails) will yield confidence $1-\varepsilon^{k\alpha_0}$ at expected cost kC_0, which satisfies the linear cost property.[5]

In the remainder of the paper, we will assume an audit scheme that has the linear cost property, that is, that the *expected* cost of auditing, *within each group* is linear *in the parameter* α_i. For schemes whose cost functions are approximately linear, our algorithm will yield a strategy that meets the required confidence level, and with cost that will typically be close to optimal. Finding the optimal-cost solution for nonlinear cost scheme will be more expensive, requiring nonlinear optimization.

If an audit scheme does not have the linear cost property, it would be fairly easy to apply our techniques using nonlinear optimization methods such as hill climbing, especially since the number of variables (i.e. the number of groups in the first-level partition of voters) is usually very small (e.g. in the U.S. Presidential election, there are 51 partitions at the lowest level). One could also approximate the cost function linearly near a proposed solution, which would lead to a correct solution (in the sense that the audit would function to guarantee the specified statistical confidence), although not necessarily a cost-optimal solution.

Because we assume the cost is linear in the α_i, we can use linear programming to find values for the α_i that minimize the total cost, subject to the constraints discussed above. For each minimal flipset F, we will have a linear constraint $\sum_{i\in F}\alpha_i \geq 1$. This will give us the optimal (lowest-cost) auditing procedure that achieves the required confidence level.

In Appendix A, we prove that two well-known ballot-based auditing methods, the Machine-assisted Election Auditing algorithm by Calandrino *et al.* [8] and the Secrecy-preserving Ballot-level Audit (SOBA) of Benaloh *et al.* [13], have the linear cost property required by our scheme.

D. Score-Based Auditing Method

In some cases, it may be difficult or inconvenient to use linear programming to find the optimal assignment of α values. As an alternative, we can approximate the solution using a score-based method that provides the required level of confidence but not a guarantee of minimal cost. To do this, we choose some method of assigning a non-negative numerical score to each group. If group i has score s_i, and if we can show that

[5] It is possible to scale to a non-integer multiple of the original α_0 and C_0 by probabilistic interpolation: if k is an integer and $0 \leq f < 1$, then an algorithm that performs the base audit k times, then with probability f performs the base audit one more time, will be linear, giving confidence $1-\varepsilon^{(k+f)\alpha_0}$ at expected cost $(k+f)C_0$.

any minimal flipset must have total score at least s_*, then we can assign $\alpha_i = \min(1, \frac{s_i}{s_*})$. (Groups that do not appear in any minimal flipset can be assigned $\alpha_i = 0$.) It is easy to show that this will be feasible, in the sense that the α values in any minimal flipset will sum to at least 1.

As an example, in a U.S. electoral vote election, we could assign each state a score equal to its number of electoral votes. If the electoral vote margin is M (that is, if at least M electoral votes would have to flip to change the election result), then it is easy to see that any minimal flipset must have total score at least $s_* = M$. Applying the score-based auditing method, a state i having e_i electoral votes gets $\alpha_i = \min(1, \frac{e_i}{M})$. The intuition is that a state's fair share of the "α burden" is proportional to its number of electoral votes.

As a refinement, we can assign $\alpha = 0$ for a subset of groups, presumably because auditing is especially expensive for these groups. We can choose a set D of groups to "drop", such that $M_D = \sum_{i \in D} \alpha_i$ is less than M. Then for every $i \in D$ we set $\alpha_i = 0$; and for every i not in D we set $\alpha_i = \min(1, \frac{e_i}{M - M_D})$. The intuition is that we don't bother to audit the groups in D, but we increase the auditing burden proportionally in the remaining groups to ensure that the total α in every minimal flipset is still large enough.

These score-based methods are likely to be useful when the number of minimal flipsets is very large. For example, in the 2008 U.S. presidential election, there are 79 841 552 minimal flipsets. Rather than enumerating them and solving a large linear programming problem, the score-based method can yield a much faster solution that we conjecture will often be close to optimal.

We observe that our score-based method is similar to the method introduced by Aslam, Popa, and Rivest [18]. That method divides votes into groups (typically precincts), but assumes that vote totals in each group are always summed to get the overall election result. We allow arbitrary aggregation rules across groups, subject to the constraint that the rules must only consider the win/loss outcome in each group. Additionally, Aslam *et al.* assume that auditing within a group is all-or-nothing: either a group is audited to 100% confidence or not at all. We admit different levels of auditing leading to different confidence intervals. Finally, our main method accounts for the bin-packing issues associated with allowing mixed confidence levels across groups, while the score-based method and the Aslam *et al.* method both ignore these issues for the benefit of ease of computation.[6]

E. Application to U.S. Presidential Elections

To illustrate the use of multi-level auditing, we can apply our method to the U.S. Presidential election from 2000 through 2012, as summarized in Figure III. As an example, the 2012 election was won by Barack Obama with 332 electoral votes, over Mitt Romney's 206. For this election, a minimal flipset would be any minimal set of states that were won by Obama and add up to at least 63 electoral votes. This calculation assumes that the expected per-ballot cost of auditing is equal in all states, so that all $c_i = 1$.

The 2000 election was very close, so there are few flipsets. Any one of the states won by Bush forms a singleton minimal flipset, so the optimal auditing strategy requires that each of these thirty states be audited to confidence level 99%. At the other extreme, the 2008 election had a larger margin of 96 electoral votes, leading to roughly 80 million minimal flipsets. Our linear program solver ran out of memory on this example, so we show a cost only for the score-based method.

F. Application to the 2010 UK Parliamentary Election

As another illustration, we applied our methods to the 2010 parliamentary election in the United Kingdom. Separate plurality elections were held in each of 565 districts. In total, members of twelve parties won seats, with the Conservative party winning 306 seats, the Labour party 258, the Liberal Democrats 57, and smaller parties winning 8, 6, 5, 3, 3, 1, 1, 1, and 1 seats, respectively. For purposes of auditing, we assume that each party's members will vote as a bloc. Since no party has a majority, a coalition of parties holding at least 326 seats in total is required to govern. We considered the set of possible governing coalitions to be the election result.

[6] While Aslam *et al.* consider linear programming as an optimal solution and give a linear program formulation of their method, they dismiss the result as necessarily too costly and complex to calculate.

Year	Electoral Vote Margin	Num. Minimal Flip Sets	Expected Number of Ballots Audited ($\varepsilon = 0.01$)			
			State-by-State	Score-Based	Score w/ Drop	Optimal (LP)
2012	63	872,775	2691.9	475.2	421.1	421.1
2008	96	79,841,552	7705.8	430.6	220.7	·
2004	17	5896	5262.6	1239.9	1239.9	1183.6
2000	2	30	64145.9	51651.1	51651.1	51651.1

TABLE III. AUDITING REQUIREMENTS FOR U.S. PRESIDENTIAL ELECTIONS 2000-2012. EXPECTED AUDITING COSTS (ASSUMING UNIT COST PER BALLOT AUDITED) REQUIRED TO ACHIEVE AN OVERALL CONFIDENCE OF 99% ($\varepsilon = 0.01$) VS. ELECTORAL VOTE MARGIN AND NUMBER OF MINIMAL FLIP SETS, AS CALCULATED USING THE OPTIMAL LINEAR PROGRAMMING METHOD, THE SCORE-BASED METHOD, THE SCORE-BASED METHODS WITH DROPS, AND A METHOD WHICH CONSIDERS AUDITING TO 99% CONFIDENCE IN EACH STATE SEPARATELY FOR THE U.S. PRESIDENTIAL ELECTIONS IN YEARS 2000-2012. FOR THE 2008 ELECTION, OUR LINEAR PROGRAM SOLVER RAN OUT OF MEMORY, SO WE SHOW ONLY THE SCORE-BASED RESULTS.

Given these assumptions, there turn out to be many possible governing coalitions that control the bare minimum number of seats. Every party can participate in such a minimum-size governing coalition. As a result, for every seat there is a minimal flipset containing only that seat, so that every seat i must be assigned $\alpha_i = 1$. Auditing to a 99% confidence level requires examining an expected 98384 ballots.

The amount of auditing required might have been much less had the election come out differently. For example, if the three major parties had gotten 256, 208, and 157 seats, and the minor parties were unchanged, then there would be only three minimal coalitions, consisting of all pairs of major parties. In this scenario the minor parties do not matter, and the smallest minimal governing coalition is a Labour-LibDem coalition with 365 seats. In this scenario, every minimal flipset involving Conservative seats contains at least 88 seats, and every minimal flipset containing Labour or LibDem seats contains at least 40 seats. Therefore we can assign every Conservative seat $\alpha_i = \frac{1}{88}$, every Labour and LibDem seat $\alpha_i = \frac{1}{40}$, and every minor party seat $\alpha_i = 0$. This would correspond to auditing every Conservative seat to a confidence level of only 0.05, and every Labour and LibDem seat to a confidence level of only 0.11. For most seats, the expected number of audited ballots would be less than one.

In general, an approach to auditing parliamentary coalition elections of this type is to compute all of the minimal coalitions (i.e., all coalitions which do not have a proper subset that is a coalition), and then to compute, for each party, the coalition containing that party which contains the smallest number of seats. Let x_i be the size (in seats) of the smallest coalition containing party i, and let x^* be the minimum number of seats needed to form a coalition (i.e., one more than half of the seats). If $w(i)$ denotes the party that won seat i, we can assign the score

$$s_i = \frac{1}{1 + x_{w(i)} - x^*}.$$

It is easy to show that any minimal flipset must have total score at least 1, so we can assign $\alpha_i = s_i$. As an additional optimization, we could consider "dropping" some seats in order to reduce the total auditing cost.

III. CONCLUSION

We introduce a novel auditing technique for examining confidence in and the integrity of real-world multi-level election systems such as the electoral college in the U.S. presidential election or coalition parliament systems in many countries.

Specifically, we describe a method for ballot-based auditing which uses the structure of the multi-level election to reduce the total amount of auditing necessary to achieve full confidence in the overall election result. We show how to use the particular structure of multi-level elections to reduce or ignore the auditing of some subgroups, reducing the cost of auditing while maintaining a defined level of overall confidence. We show both a cost-optimal approach to auditing the overall election to a specific level of statistical confidence $1 - \varepsilon^{\alpha}$ and also a score-based approximation that yields an easily computable correct, but not necessarily cost-optimal, audit strategy. We evaluate this method on real election data from the U.S. and the U.K. and show that it can significantly reduce auditing costs (in our U.S. presidential election examples, costs using our strategy were between 15.2% and 80.5% of a strategy that was independent of the election's multi-level structure; in an example drawn from

the U.K. Parliamentary election in 2010 (in which the results were highly split, allowing for many different possible coalitions), auditing to 99% confidence requires a modest cost of examining just under 100,000 ballots).

As future work, we intend to apply our frameworks to more elections and more types of election systems around the world. For example, we have only considered concretely elections where the first level in the multi-level system is decided by a majority or plurality vote. However, our results generalize readily to any selection algorithm, and we intend to consider such alternative systems in detail. For example, certain kinds of *mixed member proportional* systems (and related systems, such as those used in Germany), are not multi-level in the way we have defined. However, we believe our methods can be generalized to include such systems. We are also further refining our algorithms for determining optimal audit costs and seek to find more efficient algorithms, which are still provably cost-optimal.

APPENDIX

We give two concrete examples of multi-level election auditing using ballot-based auditing algorithms that satisfy the linear cost property. We assume in these examples for simplicity that the within-group elections are decided by a simple plurality or majority[7] and that auditing k ballots in group i has expected cost $k\ell_i$ for some group-specific expected per-ballot examination cost ℓ_i.

1) Example: Calandrino's Ballot-Based Audit: First, we give an example using election auditing algorithm of Calandrino et al. [8], which obeys the linear cost model.

Consider a group i with expected per-ballot auditing cost ℓ_i and an assigned responsibility to audit to confidence level $1-\varepsilon^{\alpha_i}$. Let m_i be the victory margin of the winning candidate. In a plurality election, $m_i = \frac{v_i^1 - v_i^2}{2}$ where v_i^1 is the winning candidate's vote count and v_i^2 is the second-place candidate's vote count. In a majority election with a winner, $m_i = v_i^1 - \frac{v_i}{2}$ where v_i is the total number of votes cast in the group. In order for the declared group winner to be wrong, at least m_i of the votes cast for the group's winning candidate must be defective, so that at least a fraction m_i/v_i^1 of the declared winner's votes must be defective. It follows that auditing n_i of the ballots cast for the group winner, without finding an error, will confirm the accuracy of the group winner with confidence level $1-(1-m_i/v_i^1)^{n_i}$, so that we can achieve the desired confidence level $1-\varepsilon^{\alpha_i}$ by setting

$$n_i = \frac{\alpha_i \log \varepsilon}{\log\left(1-\frac{m_i}{v_i^1}\right)}.$$

(If the resulting n_i is not an integer, we can interpolate: if $n_i = k+f$ for integer k and $0 \le f < 1$, we choose k ballots with probability $1-f$ and $k+1$ ballots with probability f. Then the expected number of ballots chosen is equal to $k+f = n_i$ and the other necessary properties hold.)

Applying the same argument to all groups, we see that the total auditing cost will be

$$C = \sum_i \ell_i n_i = \sum_i \ell_i \frac{\alpha_i \log \varepsilon}{\log\left(1-\frac{m_i}{v_i^1}\right)}.$$

Setting

$$\ell_i' = \frac{\ell_i \log \varepsilon}{\log\left(1-\frac{m_i}{v_i^1}\right)}$$

the cost becomes

$$C = \sum_i \ell_i' \alpha_i.$$

This is consistent with the linear-cost model.

2) Example: SOBA: To emphasize that any auditing algorithm with linear expected cost could be substituted, without changing our basic analysis, we provide a second example using SOBA [13], a modern risk-limiting audit method, which also has the necessary property that the expected cost of auditing within each group i is linear in the parameter α_i.

We assume as before that subgroup elections are decided using simple plurality or majority first-past-the-post rules and that the election in each subgroup yields a well-defined result.

Consider now group i with expected per-ballot auditing cost ℓ_i and assigned responsibility to audit to confidence level $1-\varepsilon^{\alpha_i}$. Say that the winning candidate has margin m_i Then the SOBA "diluted margin" will be m_i/N_i where N_i is the number of ballots cast in group i. That means that, given numerical parameters λ and γ,

[7] A majority election might have no winner; in that case we consider the result to be $\perp$. To simplify the exposition, we will assume in the main text that $\perp$ is not the declared result in any group, although our algorithms can easily be extended to cover that case.

the "error tolerance" and "error bound inflator", respectively, the number of ballots audited in the first round of SOBA is:

$$n_i^0 = \frac{\alpha_i}{\frac{1}{2\gamma} + \lambda \log\left(1 - \frac{1}{2\gamma}\right)}$$

SOBA proceeds by adding ballots to this sample until a specific confidence threshold is achieved. The expected additional cost from repeating the audit is negligible, scaling as C^{-2m} where C is a constant derived from the margin of victory and m is the number of misstated votes discovered [12].

The total cost C is obtained by summing over all groups gives:

$$C = \sum_i \ell_i n_i = \sum_i \frac{\alpha_i}{\frac{1}{2\gamma} + \lambda \log\left(1 - \frac{1}{2\gamma}\right)}$$

And setting:

$$\ell_i' = \frac{\ell_i}{\frac{1}{2\gamma} + \lambda \log\left(1 - \frac{1}{2\gamma}\right)}$$

we again obtain (consistent with the linear-cost model):

$$C = \sum_i \ell_i' \alpha_i.$$

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for thoughtful comments on an earlier version of this paper submitted to JETS Volume 1, Issue 1.

REFERENCES

[1] J. F. Banzhaf III, "Weighted voting doesn't work: A mathematical analysis," *Rutgers L. Rev.*, vol. 19, p. 317, 1964.

[2] L. S. Penrose, "The elementary statistics of majority voting," *Journal of the Royal Statistical Society*, vol. 109, no. 1, pp. 53–57, 1946.

[3] L. S. Shapley and M. Shubik, "A method for evaluating the distribution of power in a committee system," *American Political Science Review*, vol. 48, no. 03, pp. 787–792, 1954.

[4] K. J. Arrow, "A difficulty in the concept of social welfare," *The Journal of Political Economy*, vol. 58, no. 4, pp. 328–346, 1950.

[5] D. W. Jones, "On optical mark-sense scanning," in *Towards Trustworthy Elections*. Springer, 2010, pp. 175–190.

[6] R. T. Mercuri, "Electronic vote tabulation checks and balances," Ph.D. dissertation, University of Pennsylvania, 2001.

[7] J. A. Aslam, R. A. Popa, and R. L. Rivest, "On estimating the size and confidence of a statistical audit," in *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

[8] J. Calandrino, J. Halderman, and E. Felten, "Machine-assisted election auditing," in *USENIX/ACCURATE Workshop on Electronic Voting Technology (EVT'07)*, 2007.

[9] P. B. Stark, "Conservative statistical post-election audits," *Annals of Applied Statistics*, vol. 2, pp. 550–581, 2008.

[10] J. L. Hall, P. B. Stark, L. W. Miratrix, M. Briones, E. Ginnold, F. Oakley, M. Peaden, G. Pellerin, T. Stanionis, and T. Webber, "Implementing risk-limiting post-election audits in california," 2009.

[11] S. Checkoway, A. Sarwate, and H. Shacham, "Single-ballot risk-limiting audits using convex optimization," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT'10)*, 2010.

[12] P. B. Stark, "Super-simple simultaneous single-ballot risk-limiting audits," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT'10)*, 2010.

[13] J. Benaloh, D. Jones, E. L. Lazarus, M. Lindeman, and P. B. Stark, "Soba: secrecy-preserving observable ballot-level audit," in *Electronic Voting Technology Workship/Workshop on Trustworthy Elections (EVT/WOTE'11)*, 2011.

[14] J. Bretschneider, S. Flaherty, S. Goodman, M. Halvorson, R. Johnston, M. Lindeman, R. L. Rivest, P. Smith, and P. B. Stark, "Risk-limiting post-election audits: Why and how," Oct. 2012.

[15] D. W. Jones, "Auditing elections," *Communications of the ACM*, vol. 47, no. 10, pp. 46–50, Oct. 2004.

[16] K. Dopp, "History of confidence election auditing development (1975 to 2008) & overview of election auditing fundamentals," *National Election Data Archive*, 2008.

[17] W. R. Mebane, Jr., J. S. Sekhon, and J. Wand, "Detecting and correcting election irregularities," Stanford University, Tech. Rep., Oct. 2003. [Online]. Available: http://wand.stanford.edu/research/detecting.pdf

[18] J. A. Aslam, R. A. Popa, and R. L. Rivest, "On auditing elections when precincts have different sizes," in *USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08)*, 2008.

[19] P. B. Stark, "A sharper discrepancy measure for post-election audits," *The Annals of Applied Statistics*, vol. 2, pp. 982–985, Nov. 2008.

[20] A. D. Sarwate, S. Checkoway, and H. Shacham, "Risk-limiting audits and the margin of victory in nonplurality elections," *Statistics, Politics, and Policy*, vol. 3, no. 3, pp. 29–64, 2013.

[21] R. L. Rivest and E. Shen, "A bayesian method for auditing elections," in *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*, 2012.

[22] G. W. Cox, "Centripetal and centrifugal incentives in electoral systems," *American Journal of Political Science*, pp. 903–935, 1990.

International Standards

The Council of Europe and e-voting:

History and impact of Rec(2004)11

Robert Stein
Austrian Federal Ministry of the Interior (BM.I)
Department of Electoral Affairs
Vienna, Austria
robert.stein@bmi.gv.at

Gregor Wenda
Austrian Federal Ministry of the Interior (BM.I)
Department of Electoral Affairs
Vienna, Austria
gregor.wenda@bmi.gv.at

***Abstract*— When the Council of Europe started to deal with the subject of electronic voting in 2002, the impact of its work was not foreseeable. What followed, however, was basically a "success story": The Recommendation on legal, operational and technical standards for e-voting (Rec(2004)11), which was adopted by the Council of Ministers on 30 September 2004, has been the most relevant international document and reference regarding e-voting for a decade. Since 2010, the role of the Council of Europe with regard to e-voting has shrunk. Nevertheless various Member States expressed the desire to further review the Recommendation in the forthcoming years. Following an informal experts' meeting in Vienna on 19 December 2013, the Committee of Ministers was confronted with the suggestion to formally update the Recommendation in order to keep up with the latest technical, legal and political developments. The forthcoming Review Meeting on 28 October 2014 may help set the course for future e-voting activities of the Council of Europe.**

Keywords—Council of Europe, e-voting, internet voting, Rec(2004)11, Recommendation, review meeting, update.

I. How it started

Using technical devices in the vote casting process is no invention of the 21st century. It already started back in the 19th century [1] and some states (have) used voting machines for several decades.[1] With the rise of the World Wide Web and e-government applications in the mid-1990s, the idea of voting over the internet was born. The first binding political online election is said to have taken place in the USA in the year 2000. [2] Originally, no sharp distinction between machine voting and internet voting was drawn when employing the new term "electronic voting" or "e-voting".[2] Around ten years ago, the term "i-voting" for "internet voting" came about. [3] The interest in information and communication technologies in elections coined politicians, scientists, and administrators alike. A British opinion paper outlined the motivation for e-voting activities in 2002: "Citizens rightly expect to be able to vote in a straightforward, accessible, and efficient way, being able to have confidence in the security and integrity of the poll. (…) Governments, therefore, are being faced with requests from their citizens to introduce new technologies in the electoral processes, in particular to make available various forms of e-voting." [4] A number of international institutions and fora could have dealt with the new phenomenon of electronic voting[3] but it was the Council of Europe which apparently developed the strongest interest and formed a "multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting" within the framework of its 2002-2004 Integrated Project "Making democratic institutions work" (IP 1). The group was supported by two subgroups dealing with legal and operational aspects as well as technical aspects. [5] Some of the driving factors were the perception that citizens lost interest in politics and the drop of participation rates in elections and referenda. [6] However, Michael Remmert already noted in 2004 that "modernising how people vote will not, per se, improve democratic participation. Failure to do so, however, is likely to weaken the credibility and legitimacy of democratic institutions." [7] The Ad Hoc Group created a set of standards on e-voting, which were eventually adopted in the form of a Recommendation by the Council of Ministers on 30 September 2004. 112 legal, operational and technical standards provided valuable guidance in the new world of electronically enabled elections and gave a better idea of principles to follow and possible risks to keep in mind. Paragraph v. of the Recommendation stipulated a first review after two years "in order to provide the Council of Europe with a basis for possible further action on e-voting". Accordingly, the first review meeting was held in Strasbourg in November 2006. Since then, repeated two-year review periods were decided by all subsequent intergovernmental meetings.

II. Recommendation Rec(2004)11

Until today Rec(2004)11 is the only international document regulating e-voting from a legal perspective. Even though these

[1] In the Netherlands, all voting machines were discontinued after suspected fraud in 2007. They had been used in polling stations nationwide since 1965 (see Loeber, E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years, in Krimmer/Grimm [Eds], 3rd international Conference on Electronic Voting 2008, Proceedings [2008] 21).

[2] The term "e-enabled voting" also became more widely used.

[3] The European Union never set sustainable steps in the area of e-voting. One of the few international events was an „eDemocracy Seminar" organized by the European Commission, which took place in Brussels on 12 February 2004 and provided an overview of European e-voting activities (including the non-EU country Switzerland) at that time. The Organization for Security and Co-operation in Europe (OSCE) appointed an expert for the observation of New Voting Technologies for the first time in 2010 and developed a "Handbook for the Observation of New Voting Technologies" in 2013.

"minimal standards" are merely voluntary and thus non-binding, the member states of the Council of Europe declared their general support and commitment with the adoption by the Committee of Ministers in 2004. The Recommendation states that "e-voting shall respect all the principles of democratic elections and referendums" and "shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means." [8] Member States were asked to "consider reviewing their relevant domestic legislation in the light of this Recommendation" [9] though a wide margin of individuality was respected since individual member states were not required "to change their own domestic voting procedures which may exist at the time of the adoption of this Recommendation, and which can be maintained by those member states when e-voting is used, as long as these domestic voting procedures comply with all the principles of democratic elections and referendums". [10] Since its adoption in 2004, Rec(2004)11 has become a unique reference for matters of e-enabled voting. [11] It has been drawn upon by various countries, scientific institutions, and even courts when evaluating plans or the actual use of electronic voting. Norway is said to be the only state that incorporated most of the Recommendation's standards into the regulatory framework for the 2011 and 2013 internet voting trials. [12] A 2007 study on e-voting in Belgium, initiated by Belgian Federal and Regional administrations, took reference of Rec(2004)11 and used it as a benchmark in its evaluation. [13] The Estonian Supreme Court considered the Recommendation when deciding about the constitutionality of e-voting. [14] The 2008 pilot in Finland, where some municipalities used voting machines in polling stations, was monitored by civil society and the Council of Europe while taking Rec(2004)11 into account. [15] Switzerland had the Recommendation, as well as other practical experiences since 2004, "on the radar" when passing recent legislative changes concerning their "vote électronique". [16] In Austria, standards of Rec(2004)11 were drawn upon for the evaluation and certification of the e-voting system used in the 2009 Federation of Students' elections. OSCE/ODIHR monitored the use of "New Voting Technologies (NVT)" in a number of states in light of the Recommendation and gave respective reference in its reports. The OSCE Handbook on the "Observation of New Voting Technologies", which was published in late 2013, calls Rec(2004)11 "the only specialized international legal document in this regard" and mentions it under "Good Practice Documents" on e-voting. [17] The publication "Introducing Electronic Voting – Essential Considerations" by the International Institute for Democracy and Electoral Assistance (IDEA) listed Rec(2004)11 among the essential international documents. [18] Even in several overseas countries such as Canada [19] or the United States, [20] elements of the Recommendation were included in different studies and reports.

Despite its worldwide recognition, the Recommendation has become a bit long in the tooth. Ten years after its adoption, numerous technical developments and new social approaches have changed the "e-world". Consequently, voices in favour of a formal update have gained strength. Ongoing innovations and technological changes were already in the states' minds when a first review after two years was demanded. The e-voting group suggested to the Committee of Ministers to "recommend to member states to keep their own position on e-voting under review and report back to the Council of Europe the results of any review that they have conducted" as "e-voting is a new and rapidly developing area of policy and technology" and "standards and requirements need to keep abreast of, and where possible, anticipate new developments." [21] In 2004, the Council of Europe established a new project, "Good governance in the information society", which would last until 2010 and continued the discussions on e-voting. It also followed new challenges posed by the broader scope of "electronic democracy" (e-democracy)[4]. The overall project aimed at providing "governments and other stakeholders with new instruments and practical tools in this field and to promote the application of existing instruments and of good and innovatory policy practice". [22]

The first review meeting in Strasbourg on 23 and 24 November 2006 concluded that the Recommendation had become accepted by member states "as a valid and currently the only internationally agreed benchmark by which to assess and evaluate e-voting systems." [23] The second review meeting was organized on the occasion of the Forum for the Future of Democracy dedicated to "e-democracy" in Madrid. It took place on 16 October 2008 and summarized the latest developments and new questions concerning e-voting. In this regard, the Recommendation was still considered useful but some aspects, particularly concerning certification and observation, were identified as topics not sufficiently covered. Hence, the Council of Europe organized a Workshop on the "Observation of e-enabled elections" in Oslo on 18 and 19 March 2010 and subsequently had experts reconvene in Strasbourg in order to work on two follow-up documents complementing Rec(2004)11 – the "Guidelines on certification of e-voting systems" and the "Guidelines on transparency of e-enabled elections". [24] Both guidelines, along with an "E-voting handbook" about the "key steps in the implementation of e-enabled elections", were presented during the third review meeting in Strasbourg on 16 and 17 November 2010. This also constituted the end of the Council of Europe's activities during the project "Good governance in the information society".

III. TOWARDS AN UPDATE?

A fourth review meeting took place in Lochau near Bregenz[5], Austria, on 11 July 2012. During this meeting, several state representatives said that Rec(2004)11 was still precious but that in light of recent practical experiences, and despite the additional guidelines of 2010, a number of issues were not dealt with any more. As a consequence, the representatives of the Member States "agreed to recommend that the 2004 Committee of Ministers' Recommendation (…) should be formally updated.". [25] They further stated "that the biennial review meetings were highly useful and should be continued (…)". [26] The Republic of Austria, one of the countries actively involved in the creation of the

[4] The Council of Europe's Ad Hoc Committee on e-democracy (CAHDE) prepared a Recommendation on e-democracy (Rec(2009)1), which was adopted by the Committee of Ministers in February 2009.

[5] The precise location was Castle Hofen in Lochau near Bregenz but all international documents bear the more widely known city name of Bregenz.

Recommendation from the start, used the opportunity during the Chairmanship of the Committee of Ministers[6] to invite e-voting experts to Vienna in order to follow up and discuss the future of Rec(2004)11 within the framework of an informal workshop. Austria had already suggested such a get-together during the 2012 review meeting. [27] Since 2010, e-voting matters have not been under the umbrella of a Council of Europe project. They are now handled by the "Directorate of Democratic Governance" belonging to the "Directorate General of Democracy". The "Division of Electoral Assistance and Census" was in charge of preparing the workshop in Vienna, which was held in co-operation with the Austrian Federal Ministry of the Interior, being Austria's primary electoral management body, on 19 December 2013 in Vienna.[7] In preparation of this meeting, the Council of Europe commissioned a report "on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting". The author was Ardita Driza Maurer, an independent lawyer/consultant and former member of the e-voting team at the Swiss Federal Chancellery. [28] Based on the findings of Ardita Driza Maurer, reasons for updating the Recommendation were debated. [29] New technological developments and concepts such as in the context of the verifiability of votes, and conclusions from studies and reports, for instance regarding certification, called for addenda or adaptions (for further details on a possible future recommendation update see the article of Ardita Driza Maurer).

More than a decade ago, developing the 112 legal, operational, and technical standards was a "rather theoretically driven exercise". [30] There is no doubt that this facilitated the intergovernmental work as not too many existing systems were influenced by the then new set of rules. However, the work on the two guidelines in 2010 already showed that this situation had changed in just a few years: Since some countries meanwhile had e-voting in use or were in the process of implementing specific solutions, discussions over specific models and paragraphs became more detailed and heated than originally expected. In the end, the guidelines remained more general in their wording than intended in the beginning. The participation of civil society and other non-governmental stakeholders was also of a different quality in the early 2000s than today's era of public participation and open government would permit. Hence, the experts' workshop in Vienna concluded that "it must be ensured that the necessary legal and technical expertise is available during the drafting process and that it must be open, with detailed mechanisms to be determined, to the full range of stakeholders, e.g. civil society actors, e-voting systems providers and possibly non-member states." [31] Another difference to the drafting work of 2002 to 2004 is the monetary perpective: While the Ad Hoc Group of 2002-2004 had sufficient resources to cover travel expenses and the input of experts within the framework of Project "IP 1", no such budget is currently available at the Council of Europe. It goes without saying that proper updates could only be realized if future budgets would allow work on Rec(2004)11.

IV. Practical use of e-voting in Europe

In contrast to 2004, a number of countries have meanwhile gained experience in the e-voting field. Some of them even provide binding, e-enabled voting channels today. Other states, however, stopped using any kind of technology in the voting process. The following overview is not meant to be exhaustive but supposed to give a better feeling of some of the recent, more note-worthy activities in the field. [32]

Albania worked on two pilot projects – one regarding the introduction of electronic voter identification means in polling station (by using the national identification card), the other concerning optical scanners in two regional counting centers during the elections in June 2013. Both pilots eventually failed. In ***Armenia***, the Central Election Commission came up with a (rather simple) system allowing Armenians working at diplomatic missions abroad and Armenian professionals working for Armenian companies abroad to vote online. The legal basis was passed before the 2012 parliamentary elections but the participation rate was small. In ***Austria***, only remote voting over the internet has been seriously discussed. The Austrian Federal Ministry of the Interior conducted an intergovernmental feasibility study presented in late 2004. [33] In order to implement internet voting, an amendment to the federal constitution (two-third majority in parliament) would be required. Some non-binding academic trials [34] in 2003, 2004[8] and 2006 and a legally binding use during the 2009 elections of the Austrian Federation of Students [35] were the only notable experiences. In 2011 the Austrian Constitutional Court suspended some provisions in the regulation for the 2009 students' elections. At the same time, the Constitutional Court emphasized that in all future deployments of e-voting the legal basis had to be clearly determined in order to allow transparency both for election commissions and individual voters. [36] ***Azerbaijan*** ran some non-binding pilots of internet voting ("shadow elections") in the past but no further steps towards e-voting have materialized. ***Belgium*** did away with voting machines in the wake of the discussions in the Netherlands but has lately looked into a new and improved paper-based machine voting system which was piloted in the regional elections in October 2012 and showed the need for various modifications. The improved system is supposed to be used in half of the country during the 2014 elections. Internet voting may only be considered for Belgian voters abroad. ***Bulgaria*** started discussing e-voting solutions in both polling stations and over the internet in 2004. A draft law allowed for internet voting pilots. In 2009, a test was run in nine electoral precincts. A legal amendment on the permission of e-voting was passed in 2012 but subsequently overturned by the Constitutional Court. The current election code stipulates the introduction of machine voting in 2015. ***Estonia*** was the first

[6] Austria assumed the chairmanship of the Committee of Ministers of the Council of Europe on 14 November 2013. The formal end was the annual meeting of the Committee of Ministers on 6 May 2014.

[7] Approximately 50 persons from about a dozen countries participated, among them almost all states actively involved in e-voting (among them being Belgium, Estonia, Norway, Russia, and Switzerland).

[8] The 2004 trial was organized along the lines of the Austrian presidential elections. For further details see Alexander Prosser, Robert Kofler, Robert Krimmer, Martin Karl Unger, E-Voting Election Test to the Austrian Federal Presidency Election 2004, Working Papers on Information Processing and Information Management 02/2004 (http://epub.wu.ac.at/194/1/document.pdf).

country to introduce internet voting as a legally binding channel during the 2005 municipal elections and the 2007 parliamentary elections. [37] Online votes have to be cast in advance of the election day. [38] During the 2013 municipal elections, 24.3% of the votes came over the internet. The i-voting system and procedure are constantly improved, for instance by installing an Electronic Voting Committee composed of IT professionals responsible for conducting the i-vote process. More transparency will be ensured by introducing a new verification system, which was tested in 2013 and will become an integral part of the law in 2015. ***Finland*** piloted voting machines based in polling stations and connected to the internet in three municipalities in 2008. Following some flaws and court decisions, the project was discontinued. A working group looked into the possibilities of internet voting and presented an internal report in June 2014. Further research on the use of the internet for participative instruments was suggested. ***France*** has been using electronic voting machines in certain municipalities though the number will not be increased after the discussions in the Netherlands and Germany. Since the early 2000s, online voting for French citizens abroad had been debated and some pilots were carried out. In 2012, select representatives for the French living abroad were elected via internet for the first time. ***Germany*** used to have voting machines in certain constituencies (for all kinds of elections) since the 1960s. Due to complaints regarding the 2005 parliamentary elections, the Federal Constitutional Court of Germany held on 3 March 2009 that the use of machines undermined the principle of publicity. [39] While electronic voting machines with a paper audit trail should suffice the requirements of the decision, Germany stopped using all kinds of machines. Internet voting is exercised on a very small scale in an academic and semi-private environment but not in any political elections. ***Ireland*** introduced electronic voting machines in 2004 but never used them due to public concerns about their reliability. The machines were stored for years and finally demolished in 2012. ***Latvia*** currently focuses on the use of ITC in scanning and counting ballots. Aside from optical scanners, ideas about internet voting are debating with the neighbouring country Estonia in mind. ***Liechtenstein*** has the legal basis for e-voting in municipal elections and, influenced by developments in Switzerland, has followed e-voting discussions for a number of years – so far, however, without any further steps. ***Lithuania*** has repeatedly tried to follow the Estonian example but proposals of the Central Election Commission to introduce e-voting have not earned sufficient support in parliament yet. The Netherlands had mechanical and electronic voting machines dating back to the 1960s and also used internet voting for certain bodies. After doubts about the security of voting machines were publicly expressed by an NGO, both voting machines and internet voting were stopped in 2008 by a ministerial decree. In late 2013, a Study Commission recommended introducing electronic voting and counting "in order to make the voting and counting process more accessible and faster". Ballot stations should use new machines with ballot printers. A nation-wide roll-out could take place after a piloting phase around 2018 or 2019. ***Norway*** conducted a feasibility study on internet voting in 2006 and carried out a first pilot on the local level (10 municipalities and 4.5 % of population) in 2011. Lessons learned from other e-voting examples, for instance the need of universal verifiability, were taken into consideration. Another use of internet voting took place during the 2013 parliamentary elections (12 municipalities and 7% of population). In June 2014 the government announced to discontinue the use of e-voting trials. [40] In ***Russia***, the Central Election Commission introduced electronic voting machines with a paper audit trail in 2005. In February 2013, the constitutional committee proposed to look into internet voting as well. In Slovenia, electronic voting machines have been used in polling stations in order to assist handicapped voters though no further expansion seems to be considered. In ***Spain***, pilots regarding electronic voting machines have been carried out since 1995. In addition, some internet voting tests were carried out on the regional (2003, Catalonia) and national level (2005). The basis for internet voting was laid down in the Basque Country electoral code in 1998. Lately, no further serious discussions have materialized. ***Switzerland*** had its first debates on internet voting in 1998 and started a pilot project on e-voting ("vote électronique") in three cantons in 2002. In the beginning, it was only used in local elections and referenda. In 2011, the first nation-wide use (for national parliamentary elections) took place. The government is still in the process of gradually expanding the use of e-voting. New legal backbones for the federal level were adopted in December 2013. In order to further extend internet voting, a new model of verifiability and new auditing routines will be required. Until the end of 2013, 12 cantons used e-voting in one way or the other. The ***United Kingdom*** was very active in testing all kinds of electronic voting methods in the early 2000s. Trials in several constituencies between 2002 and 2007 involved ballot booth voting, kiosk voting, and internet voting. After negative experiences in other countries and critical voices from the UK Electoral Commission, [41] the government has not looked into e-voting opportunities any further. In March 2014 the chair of the UK Electoral Commission called for a modernization of elections and a move to online voting. [42]

Interesting enough, the implementation of the European Citizens' Initiative[9] in all EU Member States on 1 April 2012 recently stirred up discussions about new forms of e-participation in several member states since it is possible to sign a statement of support online. [43] The future will show whether this new instrument of direct democracy in the EU really has an impact on e-voting discussions around Europe.

V. Outlook

The future of e-voting certainly looked brighter when Rec(2004) 11 was adopted ten years ago. While e-enabled elections were still in their infancy, some kind of "e-voting hype" seemed to go around, which led to legal amendments or the first pilots in a number of countries. [44] In the meantime, some kind of stagnation has emerged [45] though current international examples show that electronic voting is possible – not only in a supervised environment but also with online solutions. [46] The reasons for a decline of the e-voting euphoria are multifaceted. The economic and financial crisis of

[9] Regulation (EU) No 211/2011 of the European Parliament and the Council of 16 February 2011 on the citizens' initiative.

2008 led to budget cuts in several countries; expensive innovation programs had to be stopped. Strict court decisions concerning the use of e-enabled voting [47] as well as a growing distrust of citizens in internet solutions after data leak and hacking incidents also did their bit. Concerns about security and reliability problems inherent to online applications were already present when passing Rec(2004)11, which states "(…) that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting." [48] Today it is mainly a political decision whether countries are willing to think about e-enabled voting as computers and the internet have already influenced our daily life in an unprecedented way. Permanently excluding modern technology from voting and participative instruments does not appear realistic.[10]

The Council of Europe continues to be the only organization in Europe to set intergovernmental standards in the field of e-voting. Accordingly, the informal experts' meeting in Vienna in December 2013 (similar to the 2012 review meeting) came to the conclusion that, (…) "taking into account the issues listed in this report and the high probability that in the medium and long term, the number of electoral systems will comprise some electronic features, there are a number of strong and valid reasons for updating Recommendation Rec(2004)11." The exact terms of such an update were left to the Council of Ministers, which debated the report in the Ministers' Deputies/Rapporteur Group on Democracy (GR-DEM) on 20 May 2014 but rendered no final decision. Even the definite organization of another review meeting by the Council of Europe Secretariat in late 2014 remained uncertain at that point of time. Thus Austria, along with Belgium, Estonia, Hungary, Latvia, Poland and Switzerland, sponsored a "non-paper" for information "in view of the meeting of the GR-DEM on 17 June 2014" in order "to call for the 5th Review Meeting to take place in Autumn 2014". The delegations emphasized that such a meeting could be organized "on a costs-lie-where-they-fall basis" to keep expenses "to an absolute minimum". The non-paper also suggested that the review meeting could be held back to back with the EVOTE 2014 conference in Lochau, Austria, to take advantage of the obvious synergies.

The Council of Europe Secretariat confirmed its support of the proposal in the GR-DEM meeting on 17 June 2014 and stated that the results of such a review meeting could even feed directly into relevant discussions at the World Forum for Democracy.[11] Official invitations for the 5th meeting "to review developments in the field of e-voting since the adoption of Recommendation Rec(2004)11", scheduled for 28 October in Lochau, were sent out by the Democratic Governance Directorate of the Council of Europe on 23 June 2014. The agenda contains the points "Horizon 2016: General exchange of views on a possible update of the CM Rec(2004)11 - defining the scope of a possible update" as well as "discussion of possible first elements of the future updated Rec(2004)11 and necessary conditions for the next steps: modus operandi, terms of reference, possible timeline". There is no denial that the Council of Europe's expertise and reputation in electronic voting is internationally renowned. The Recommendation, its review, and the general objective of developing secure use of the internet in the field of democratic elections currently form part of the Council of Europe's Internet Governance Strategy 2012-2015. [49] However, future activities will largely depend on the allocation of the essential budget. It will be up to the Committee of Ministers to say which role the Council of Europe wants to play in the area of e-voting in the future. In case of a "go" for a formal Recommendation update, its outstanding role in this matter would be re-iterated.

[10] In countries with multiple voting channels such as postal voting, the free selection of polling stations or mobile election commissions, the pressure to introduce e-voting does not seem to be as strong as in those countries where the present voting system is less flexible.

[11] To be held in Strasbourg on 3 to 5 November 2014 (http://www.coe.int/de/web/world-forum-democracy).

REFERENCES

[1] Krimmer, Overview, in Krimmer (Eds), Electronic Voting 2006, 2nd International Workshop Proceedings (2006) 9.x

[2] Barrat i Esteve/Goldsmith/Turner, International Experience with E-Voting, Norwegian E-Vote Project, IFES Study (2012) 1.

[3] Inter alia, Buchsbaum, Aktuelle Entwicklungen zu E-Voting in Europa, JRP 2004, 106; Grabenwarter, Briefwahl und E-Voting: Rechtsvergleichende Aspekte und europarechtliche Rahmenbedingungen, JRP 2004, 70; Stein/Wenda, E-Voting in Österreich, SIAK-Journal 3/2005, 3.

[4] IP 1 : Exploratory Workshop on e-voting (1-2 July 2002), Proposal for a Council of Europe activity on e-voting standards - document prepared by the United Kingdom authorities (http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Work_of_e-voting_committee/03_Background_documents/98IP1(2002)11_en.asp#TopOfPage).

[5] All meeting reports are available online: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Work_of_e-voting_committee/02_Agendas_and_Reports/Default_en.asp#TopOfPage

[6] See introduction on the CoE website on the E-Voting Project: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/

[7] Remmert, M. (2004), "Towards European Standards on Electronic Voting", in Prosser, A. and Krimmer, R. (Eds.), Electronic Voting in Europe - Technology, Law, Politics and Society, P-47, Gesellschaft für Informatik, 15.

[8] Rec(2004)11, Preamble, Paragraph i.

[9] Rec(2004)11, Preamble, Paragraph iii.

[10] Rec(2004)11, Preamble, Paragraph iv.

[11] For further details see Maurer, Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 29 November 2013.

[12] http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_relating_to_trial_internet_voting_2013.pdf

[13] http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf

[14] Madise, Ü. and Vinkel, P. (2011) "Constitutionality of Remote Internet Voting: The Estonian Perspective", Juridica International. Iuridicum Foundation, Vol. 18, 4–16.

[15] Whitmore K., Congress of Local and Regional Authorities (2008) Information Report on the Electronic Voting in the Finnish Municipal Elections, https://wcd.coe.int/ViewDoc.jsp?id=1380337&Site=Congress

[16] Concerning e-voting in Switzerland see: http://www.bk.admin.ch/themen/pore/evoting/

[17] OSCE, Handbook for the Observation of New Voting Technologies (2013) 8.

[18] http://www.idea.int/publications/introducing-electronic-voting/loader.cfm?csmodule=security/getfile&pageid=47347 (published in 2011).

[19] Schwartz, B. and Grice, D. (2013) Establishing a legal framework for e-voting in Canada, http://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf

[20] U.S. Election Assistance Commission (2011) A survey of Internet Voting, http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

[21] Remmert, M. (2004) "Towards European Standards on Electronic Voting", in Prosser, A. and Krimmer, R. (Eds.), Electronic Voting in Europe - Technology, Law, Politics and Society, P-47, Gesellschaft für Informatik, 14.

[22] CoE website: http://www.coe.int/t/dgap/democracy/Activities/GGIS/Default_en.asp

[23] CoE website: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/

[24] Wenda, „Good Governance in the Information Society" – Der Europarat und E-Voting, in Schweighofer/Kummer (Hrsg), Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts, Tagungsband des 14. Internationalen Rechtsinformatik-Symposions IRIS 2011 (2011) 293 ff.

[25] Report Fourth Review Meeting, 4 June 2013, DGII/Inf(2013)06, 5.

[26] Report Fourth Review Meeting, 4 June 2013, DGII/Inf(2013)06, 6.

[27] Report of the Fourth Review Meeting of 4 June 2013, DGII/Inf(2013)06, 5 ("… it should be noted that a number of member states represented at the review meeting [including Austria, which will hold the Chairmanship of the Committee of Ministers from November 2013 to May 2014] might be willing to consider making some extra-budgetary voluntary contributions to facilitate and expedite this work.")

[28] Maurer, Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 29.11.2013.

[29] For a summary of the whole debate see Report of 25 April 2013, DGII/Inf(2014)06, 4-6.

[30] Report of 25 April 2013, DGII/Inf(2014)06, 4.

[31] Report of 25 April 2013, DGII/Inf(2014)06, 5.

[32] Sources of this summary include the relevant OSCE/ODIHR Reports, the proceedings of the EVOTE 2012 Conference near Bregenz, Austria, the Workshop Report of 25 April 2013, DGII/Inf(2014)06, 2-6, and notes of Robert Krimmer (ODIHR's expert on New Voting Technologies from 2010-2014).

[33] http://www.bmi.gv.at/cms/BMI_wahlen/wahlrecht/E_Voting.aspx

[34] Prosser, A., Krimmer, R., Kofler, R. Electronic Voting in Austria. Current State of Public Elections over the Internet, in: Kersting, Norbert, Baldersheim, Harald (eds): Electronic voting and democracy. A comparative analysis. New York (2004).

[35] For further details, see the evaluation report: http://www.e-voting.cc/wp-content/uploads/downloads/2012/05/Evaluierungsbericht_E-Voting_Hochschuelerinnen-_und_Hochschuelerschaftswahlen_2009.pdf

[36] http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/6/7/CH0006/CMS1327398738575/e-voting_v85-11.pdf

[37] Trechsel, Alexander H. et al., 2007. Internet Voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe. Strasbourg, Council of Europe (2007).

[38] http://www.vvk.ee/voting-methods-in-estonia/engindex/

[39] http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html

[40] http://www.regjeringen.no/nb/dep/kmd/pressesenter/pressemeldinger/2014/Ikke-flere-forsok-med-stemmegivning-over-Internett-.html?id=764300

[41] http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/KeyfindingsandrecommendationssummarypaPer_27191-20111__E__N__S__W__.pdf

[42] http://www.theguardian.com/politics/2014/mar/26/uk-e-voting-elections-electoral-commission-voters

[43] Inter alia, Stein/Wenda, Implementing the ECI: Challenges for the Member States, in Prosser (Eds), EDEM 2011, Proceedings of the 5th International Conference on E-Democracy (2011) 45.

[44] Inter alia, Kersting, Norbert, Baldersheim, Harald (eds): Electronic voting and democracy. A comparative analysis. New York: Palgrave (2004).

[45] Inter alia, R. Michael Alvarez & Thad E. Hall, Electronic Elections: The Perils and Promises of Digital Democracy (2010).

[46] See, inter alia, Barrat i Esteve/Goldsmith/Turner, International Experience with E-Voting, Norwegian E-Vote Project, IFES Study (2012) und den Bericht des „Fourth Review Meeting" vom 4. Juni 2013, DGII/Inf(2013)06, 2 ff.

[47] See especially the German Federal Constitutional Court ruling of 3 March 2009, http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html and the Austrian Constitutional Court ruling of 13 December 2011, http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/6/7/CH0006/CMS1327398738575/e-voting_v85-11.pdf

[48] Rec(2004)11, Preamble.

[49] CM(2011)175 final of 15 March 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internet%20Governance%20Strategy/Internet%20Governance%20Strategy%202012%20-%202015.pdf

Ten Years Council of Europe Rec(2004)11

Lessons learned and outlook

Ardita DRIZA MAURER
Jurist, Ll.M., Consultant
Switzerland
info@electoralpractice.ch

***Abstract*— E-voting must comply with requirements for democratic votes and elections. Adopted in 2004, the Council of Europe Recommendation Rec(2004)11 is one of the first regulatory efforts in this area and so far the only one at the international level. Its ambition is to map legal principles for democratic elections with operational and technical requirements specific to e-voting. This paper presents an overview of lessons learned from the application of the Recommendation during the past ten years and discusses the need for an update.**

Keywords—Council of Europe, e-voting, regulation, Rec(2004)11, recommendations, update

I. INTRODUCTION

The Recommendation of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, also known as Rec(2004)11 [17], was adopted on 30 September 2004 by the Committee of Ministers which also took note of the Explanatory memorandum thereto [18]. Both documents were compiled by a Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting.

The Recommendation defines e-voting as an e-election or e-referendum that involves the use of electronic means at least in the casting of the vote, covering both e-voting in controlled (e.g. voting machines in polling stations) and in uncontrolled environments (e.g. internet voting from a private computer). Rec(2004)11 became rapidly a reference for Council of Europe (CoE) States that introduce or envisage introducing e-voting[1]. It remains so far the only international instrument to propose an e-voting regulation.

Two additional instruments [14][15] were adopted in 2010, however with the lower status of guidelines. They propose guidance on certification and transparency issues and are meant to complete the recommendations on these issues[2]. A formal proposal to update the Recommendation was introduced in the 2012 review meeting. The issue of an update is on the agenda of the 2014 review meeting[3].

This paper reflects on the necessity of updating Rec(2004)11 based on e-voting experiences and the use of the Recommendation in the past ten years in the CoE region. The main arguments in favour of an update include lessons learned by experimenting with e-voting or by observing it, critical assessments of the Recommendation as well as technical developments (section 2). A possible line for approaching the update is presented by way of conclusion (section 3).

The paper is based on our report to the Council of Europe on the possible update of the Recommendation [19]. The report was discussed at a CoE's organized meeting of experts in Vienna (19 December 2013). Findings are grounded mainly on the documents of the four CoE biennial review meetings that took place since its adoption, on e-voting regulations and evaluations (e.g. by countries, by international organizations, etc.) and on e-voting related work by organizations or countries beyond the CoE region. The paper focuses on e-voting regulatory issues alone.

II. LESSONS LEARNED

A. The special place of Rec(2004)11

A recent study [2] mentioned that emerging international electoral standards on e-voting are struggling to catch up with the introduction of technology into the voting and counting process. This could also apply to Rec(2004)11.

The starting point for introducing the Recommendation in 2004 was the observation that member states are already using, or considering using e-voting for a number of purposes (see the Preamble). Ten years later, OSCE/ODIHR [34] observed that today, almost all electoral processes make some use of new technologies from voter registration to tabulation of results.

Regulating e-voting is a challenging task and countries look for guidance. The Recommendation timely responded to such needs, rapidly becoming a reference (see also [27] on the

[1] Country reports presented at the CoE biennial meetings on e-voting (see http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Default_en.asp) reflect the implementation of the recommendations by countries. U.S. EAC 2011 report on internet voting found that in particular internet voting systems were either conceived or updated by incorporating the CoE Recommendation.

[2] Transparency is dealt in paragraphs 20 to 23 (Appendix I) and certification in paragraphs 111 and 112 (Appendix III) of the Recommendation.

[3] A fifth review meeting on the Recommendation organized by the Council of Europe will be held on 28 October 2014 in Lochau/Austria, back to back with EVOTE 2014.

role of Rec(2004)11 in fostering e-democracy). It is still the only international instrument to propose standards for regulating remote and non remote e-voting. The adoption of common standards in the Recommendation was considered key to guaranteeing the respect of all the principles of democratic elections and referendums when using e-voting [18] [37].

A number of organisations have produced guidelines on the introduction of new technologies in voting. The OSCE/ODIHR [34], IDEA [5] the Carter Center [10], the Organization of American States [33] and the National Democratic Institute for International Affairs [35] have approached the issue of standards for electronic voting and counting technologies from the perspective of election observers. IFES [24] proposes a step-by-step approach to the introduction of e-voting, including legal considerations. IFES [45], IDEA [25] or the EU [23] discuss key principles that should inform the introduction of e- voting or more generally of technology in elections. The Council of Europe also developed a Handbook [16] to provide guidance on the steps to be considered when introducing e-voting.

These documents focus on identifying good practices or formalizing procedures. They do not aim at providing an e-voting regulation and most of them are domain specific focusing on the needs of election officials, observers and so on. They need to be taken into account when updating the Recommendation but they are not equivalent to it (e.g. in their respective scopes) and no substitute to it. One explanation to that may lie in the fact that no other institution has a mandate equivalent to the CoE in setting electoral standards, at least in Europe[4].

Rec(2004)11 has also been referenced by countries and organizations beyond the CoE region when considering e-voting regulations or standards. A study commissioned by Elections Canada [39] considers the work done by CoE in this field as the most extensive while creating a legal framework for a new technology. It recommends election officials to consider referencing the Rec(2004)11 check-list. The U.S. Electoral Assistance Commission [40] has referenced the Recommendation in an effort to locate standards and requirements on internet voting utilized elsewhere in the world which include voting specific functionality, accessibility and security requirements.

B. Guiding principles or detailed requirements?

Rec(2004)11 is a pioneer effort which attempts to apply a finite but not consolidated number of legal requirements for democratic elections, dispatched in a set of international instruments only some of which are mentioned in the Preamble of the Recommendation, to e-voting.

The Recommendation is a non-mandatory instrument despite the fact that it has been accepted unanimously by the Council of Ministers and it says that member states should consider reviewing their relevant domestic legislation in the light of this Recommendation when introducing e-voting (recommendation iii). Furthermore the text of the Recommendation and of the Explanatory Memorandum itself imply that the recommendations are not exhaustive. However, in several cases, the Recommendation has been considered as a ready-to-use check-list of requirements for building and evaluating e-voting systems. Whether the Recommendation is ready for this use is questionable.

Since the first review meeting in 2006 it has been reconfirmed that the Recommendation was accepted by member States as a valid benchmark by which to assess and evaluate e-voting systems. At the same time it has been admitted that several issues, such as accreditation, certification or observation needed further research. The two guidelines on certification and transparency were endorsed as providing a common reference to be viewed, however, as work in progress since the practical experiences in the field of e-voting were in constant evolution. The last 2012 review meeting concluded that existing loopholes, ambiguities or tensions in the Recommendation justify a formal update.

Norway is the only country to have given Rec(2004)11 recommendations (with few exceptions however) the status of legal basis regulating both 2011 and 2013 internet voting trials [31][32]. However some of the recommendations were excluded and Norway also introduced verification mechanisms which are not dealt with in the Rec(2004)11 such as return codes [4].

The Norwegian system has been evaluated [1] for its conformity to Rec(2004)11 (see also [3]). The evaluation [1] concludes that as a package, the Council of Europe Recommendations represent a very comprehensive and detailed set of standards for the conduct of electronic voting. The Norwegian Internet voting system was found compliant with 85 out of the 102 relevant recommendations and non-compliant with three recommendations. This was considered a significant achievement given the exacting nature of the Council of Europe Recommendations. The difficulties encountered in applying the requirements of Rec(2004)11 prompted the authors to present a critical assessment of the recommendations.

The study [1] concluded that the Recommendation does not build on existing public international law, that it says little on the legal basis, that it aims at designing standards applicable to all circumstances and such a broad scope is problematic when it comes to their implementation, that it ignores the fact that trade-offs between standards are sometimes necessary in electronic voting (such as the need for secret voting against the need for transparency, and the need to be able to audit the function of the voting system), that the need to comply with the Recommendation as a whole is problematic, that a number of standards may appear to be overlapping or redundant, that the wording is sometimes vague (interpretation is needed) and other times too detailed and, finally, that the recommendations are technically neutral

[4] According to article 1 of the 1949 adopted Statute of the Council of Europe the organization has the aim to achieve a greater unity between its members for the purpose of safeguarding and realising principles which are their common heritage. This aim shall be pursued by agreements and common action in legal and administrative matters. Article 15 of the CoE Statue foresees that action may take the form of recommendations to the governments of members. Available: http://conventions.coe.int/Treaty/en/Treaties/Html/001.htm

in their wording, but not in their consequences when attempting to comply.

Similar critiques on the wording and structure of Rec(2004)11 were also issued earlier in two theoretical analysis of the Recommendation [26], [30]. Without considering the merits of the standards included in the Recommendation, [30] employed engineering requirements and reverse engineering techniques to show that standards are expressed in a poor way and to make a first, simple, restructuring of the Recommendation. Considering the Recommendation as a check-list of requirements for system certification purposes, the study concludes that the Recommendation as it stands makes certification against standards difficult. Several "original flaws" are identified including inconsistency, incompleteness and unclear scope, over-specification, under-specification, redundancy and repetition as well as maintainability and extensibility issues. The authors believe that a broadly applicable instrument would be genuinely useful both to governments procuring e-voting systems, and to vendors developing and maintaining such systems. So they undertake a first-step restructuring of the Recommendation, rooting out the identified original flaws.

Another study on a concrete use of the Recommendation [20] questioned the possibility for Rec(2004)11 to handle sufficiently real-world attacks against elections using e-voting. Under this perspective the Recommendation was considered as being (or ought be) specific enough as to provide detailed solutions to deal with specific threats such as skilled, creative, personally motivated and appropriately equipped students planning and executing attacks against e-voting systems. The authors propose that Rec(2004)11 be further improved by explicitly pointing out the necessity of implementing adequate countermeasures to different types of attacks and that the development of a special security strategy to deal with attacks that target voters' acceptance of e-voting should be recommended in Rec(2004)11.

The discussion on the adequacy of national regulations to cover current forms of e-voting and the required level of detail of such regulations is informative also for Rec(2004)11 given the similar challenges that all regulations face. The German Constitutional Court considered in its 2009 decision [8] that the Federal Ordinance on the Deployment of Voting Machines in Elections was unconstitutional because it did not contain provisions ensuring that only those voting machines are approved and used which comply with the constitutional preconditions of the principle of the public nature of elections (see paragraph 145 and ff. of the Court's decision) which requires that each voter, without any specific technical knowledge, is able to make sure that the system performs correctly.

The Austrian Constitutional Court in its 2011 decision [42] arrived at a similar conclusion, although based on different principles. The act regulating the elections of the Students' Union was found to be unconstitutional because it did not provide detailed requirements on the e-voting system and on the procedures to ensure that competent authorities could exercise their controlling rights. Both the German and the Austrian quashed regulations have not been updated since.

The Estonian Constitutional Judgement of the Supreme Court of 2005 [38] examined the e-voting legal basis only from the point of view of the principle of constitutionality in relation with the right to change a vote in the internet voting context alone. The Court explained that the right to change the e-vote is in accordance with the CoE Recommendation [29] and with the Estonian Constitution.

The adequacy and level of detail of national e-voting regulations have been discussed elsewhere as well. Belgium Federal and Regional Administrations commissioned a thorough study on e-voting [6] which considers Rec(2004)11 as the main benchmark for evaluating e-voting.

Finland's use of voting machines in polling stations was monitored in the light of Rec(2004)11 by both Electronic Frontier Finland [21] - a Finnish non-profit - and the Council of Europe, Congress of Local and Regional Authorities [44].

France's non-remote e-voting is regulated by specific legislation while remote internet voting, must comply with recommendations by the National Commission on Informatics and Liberties [12] whose structure and content presents many commonalities with Rec(2004)11. A recent thorough report [11] recommended that the list of legal requirements for authorizing the use of voting machines must be completed (recommendation 2).

Netherlands discontinued all forms of e-voting because, in addition to computer security problems, the embedding of the voting machines within the legal framework was considered very weak. Another lesson from the Netherlands is that technical choices made in the past to embed basic principles of elections need to be periodically reconsidered [28].

Swiss federal legislation on e-voting from uncontrolled environments introduced in 2002 presented many commonalities with Rec(2004)11 [7]. The Federal Ordinance[5] was recently modified to reflect lessons learned during the past ten years [13] and was completed with a detailed technical regulation[6].

To conclude, the scope and aim of the Recommendation need to be clarified. While Rec(2004)11 was initially intended to provide guidance, it has in several occasions been referred to as a complete and comprehensive list of requirements against which to evaluate e-voting systems. As a guiding document the Recommendation is sometimes too detailed and when considered as a take-it-or-leave-it check-list of requirements its application has proved difficult.

Furthermore the level of detail of the Recommendation requires special attention. In the light of experiences made and lessons learned so far it can be assumed that a readily implementable check-list of requirements will receive greater attention. It should be comprehensive and coherent to facilitate implementation and control. It should at least contain necessary requirements to ensure compliance of e-voting with

[5] In force since 15 January 2014, http://www.admin.ch/opc/fr/classified-compilation/19780105/index.html

[6] In force since 15 January 2014, the technical regulation is a Federal Chancellery Ordinance: http://www.admin.ch/opc/fr/classified-compilation/20132343/index.html

all international standards for democratic elections while leaving individual countries the necessary room for implementing their own electoral specificities.

C. Placing e-voting into its context

Reference [26] found it problematic that requirements (mainly security requirements) for e-voting are measured (*as secure as*) against requirements for non-electronic voting systems. As there exist no widely accepted metrics for measuring, reasoning by analogy flaws the comparison between the two. This critique needs to be addressed in a future update.

Reference [26] also draws attention to the necessary distinction between matters of public policy which affect the whole electoral system and matters of voting technology when introducing recommendations. The following example from the implementation of the Recommendation illustrates this.

In some cases, the same recommendation is implemented in opposing ways by different countries in accordance with their own specificities. This is the case with "secrecy and freedom of the vote" (recommendations 9 to 19). Norway and Estonia introduced multiple voting, or the right to change the e-vote for internet voters alone and a precedence of paper ballots over electronic ballots. This was meant to offer the voter a way to get around voting coercion and vote buying (which may arise in remote voting, because the voter can be forced to cast his or her vote in the presence of another person). Although multiple voting literally contradicts recommendation 5, [4] and [38] found that this may be interpreted to respect the Recommendation. France and Switzerland do not allow multiple voting and assign the same value to a validly issued ballot, be it on paper or electronic. Their point of view is that internet voting is just another form of distant voting from an uncontrolled environment, and that coercion will not be addressed differently for internet voting than for postal voting. ODIHR[7] encourages France and Switzerland to introduce multiple voting but says nothing of the impact this would have on the system as a whole given the inequality it will create with other channels and the fact that not all voters have access to internet voting.

The national legal context should be taken into account when regulating e-voting. Some issues may only concern e-voting. Others, although introduced in an e-voting context, are a matter of public policy (for example related to remote voting) not of voting technology. Their introduction will affect the whole system. Furthermore the technical dimension of e-voting is important and should be kept in mind when regulating it. Reasoning by analogy with postal voting has serious limits and must be used with care.

D. Same provisions for different e-voting systems?

Rec(2004)11 applies a number of legal requirements for democratic elections to an indefinite number of voting solutions, collectively known as remote and non-remote e-voting, that only share one common characteristic: the use of electronics in casting the vote. As the above mentioned analysis of the conformity of the Norwegian system showed, several recommendations are clearly written with non-remote e-voting in mind and have proved difficult to implement in an internet voting context.

Requirements and standards in the Recommendation should clearly indicate to which of the two types of e-voting they apply. Venice Commission [22] stated that e-voting in supervised environments must be treated differently from e-voting in unsupervised environments. In particular, the issues of secrecy and freedom of the vote are to be handled differently in the two cases. So, a prior determination when updating the Recommendation should be clearly to distinguish between the two categories. There is general consensus on this admitted conclusion and it was included in the report of the Rec(2004)11 review meeting of 2012 as well.

E. Technology developments, new concepts and solutions

As indicated by its title, the Recommendation is multi-disciplinary and requires combined expertise from different areas. Important work has taken place on the technical aspects of e-voting such as e-voting protocols, e-voting control and certification or e-voting increased transparency through cryptographic solutions[8]. Their consideration in the light of Rec(2004)11 goes beyond the scope of this paper. However their significance for the Recommendation needs to be examined in view of an update.

An interesting example from a regulatory perspective is work on certification [43] as it illustrates the impact legislation has on the design and control of e-voting systems. The broad principles mentioned in Appendix I of the Recommendation serve as legal background. Based on them, detailed security requirements and methods to measure and evaluate e-voting systems' security have been developed. They must be considered in view of an update of the recommendations, namely those contained in Appendixes II and III.

OSCE/ODIHR has monitored the use of e-voting in elections in different CoE countries. Its reports provide valuable information on the implementation of the Recommendation (which serves as a legal benchmark) as well as on the legal frameworks for e-voting in different countries[9]. ODIHR often gives substance to high-level requirements. Its 2013 published Handbook for the observation of new voting technologies includes a collection of such detailed recommendations. However the leap from the general OSCE and Council of Europe requirements to specific

[7] See OSCE/ODIHR'S 2012 reports on both countries' parliamentary elections, http://www.osce.org/odihr/elections

[8] Proceedings of periodical conferences such as Bregenz EVOTE, EVT/Wote, and Vote-ID give a good overview of such developments. See the respective websites: http://www.e-voting.cc/en/publications/proceedings/ ; https://www.usenix.org/conference/evtwote ; http://www.voteid13.org/

[9] OSCE/ODIHR has reported on the use of new voting technologies in several countries in the region and beyond, including Norway 2013, U.S.A. 2013, France 2012, Norway 2012, Switzerland 2012, Russian Federation 2012, Estonia 2011, Belgium 2007, Estonia 2007, Finland 2007, Kazakhstan 2007, the Netherlands 2007, Belgium (Expert Visit on New Voting Technologies) 2006, Kazakhstan 2006. All reports can be retrieved from http://www.osce.org/odihr/elections

recommendations such as those on introducing verifiability in e-enabled elections, is somewhat huge and only based on the even-less-mandatory Guidelines on transparency[10].

Several new concepts have been discussed and even introduced in the past ten years in e-voting. Most of them aim at ensuring transparency and fostering trust and confidence in the e-voting channel and are reflected in the Guidelines on transparency. Such concepts include "the use of a second medium to store the vote to improve transparency", the related "mandatory count of the second medium in a statistically meaningful number of randomly selected polling stations", specific "rules dealing with discrepancies between the mandatory count of the second medium and the official electronic results", the requirement to "gain experience in providing mechanisms that allow voters to check whether their vote was counted as intended" (paragraphs 13 to 16 of the Guidelines). Also the concept of "chain of trust in e-enabled elections" according to which voters should be able to verify if their e-vote was cast as intended, recorded as cast and counted as recorded has been implemented, introducing a new possibility for the voter to prove that their own single e-vote was cast as intended, recorded as cast and counted as recorded.

Although inspired by traditional voting, these mechanisms are new to electoral legislation. They are specific to e-voting and appear today as necessary to ensure that the public can place the same trust in e-voting as in other non-electronic voting systems. As usual with experiments, practice has so far preceded regulation. However we are now at a point where there exists a certain consensus on their use and they are being introduced in a number of countries[11]. Such new concepts and mechanisms being legally relevant, they need to be defined and their use regulated by law. The general requirements of transparency in the Recommendation and Guidelines do not regulate their implementation, operation, and control.

In addition to new concepts, our understanding of existing concepts has evolved. Experience with e-voting machines in the U.S.A. for instance shows that while voting system standards and certification against standards are useful for examining the basic aspects of voting machines, they cannot ensure secure voting systems, security being a negative quality [9]. A recent report [36] recommended reforming the certification process and conducting systematic after-election-auditing of voting equipment. Similar arguments are heard in Europe as well where the cost-efficiency of certification has been questioned and individual and universal verifiability is seen as offering better guarantees while at the same time being less costly than certification.

In the light of the previous examples and given the recognized position of the Recommendation in the regulatory field, it is necessary that Rec(2004)11 be updated to take into account technology developments and current practices.

III. UPDATE OF REC(2004)11

As with other technology related developments, e-voting regulation is being adjusted as technology advances and our understanding of it improves. In order to provide basic guidance for countries and also ensure that Council of Europe's electoral heritage is integrated in a coherent way in e-voting regulations by countries, the Recommendation needs an update in the light of recent developments and experience gained. Below we will present some thoughts on how to tackle the updating work.

A. Prior determinations

Compared to a similar document, the U.S. Voluntary Voting System Guidelines (VVSG) [41], the structure and language of Rec(2004)11 is very different. Both are voluntary. However, if adopted, VVSG provides a check-list ready for use by authorities, vendors, certifying bodies, etc., while Rec(2004)11 was intended to provide guidance, although some parts of it are too detailed for such a purpose.

Before undertaking a thorough update of the Recommendation, a decision has to be made on the kind of document we want. It can be assumed that a readily implementable (by authorities as well as by industry) check-list will receive greater attention. This decision will influence the structure, content, level of detail and wording of the entire Recommendation.

As mentioned earlier the level of detail requires attention. A detailed Recommendation may be interesting as countries look for guidance. However, the higher the level of detail, the greater the probability that the Recommendation cannot apply 100% in a specific case. A solution could be to adopt a modular approach, instead of the current situation which requires that the Recommendation be applied as "one block". The modular approach implies a mandatory layer of recommendations (minimum standards applicable everywhere in the region) on which modules of additional, optional standards would be build. Both a generic document and a more detailed one are possible choices for the Recommendation. Both require a good interleaving of legal, operational and technical requirements. Once the level of detail has been decided, it has to be applied coherently throughout the document.

Another prior determination would be clearly to distinguish recommendations dedicated to e-voting in controlled (polling stations) or in uncontrolled (remote voting) environments.

The Recommendation and the two Guidelines were developed separately (respectively in 2004 and 2010) and have different legal value. However they are closely linked to each other. Consolidating the three documents (merging, simplifying and streamlining) may be necessary.

In a second step, consideration may be given to a possible separation of hard-core requirements from more rapidly changing ones. Such a trend is observed in other similar

[10] Examples include the recommendation in 2007 that Belgium introduces legislation on voter verified paper audit trail (VVPAT) or an equivalent verification procedure and the recommendation (2012) to France and Switzerland to consider the use of a verifiable internet voting scheme or an equally reliable mechanism for voters to check whether or not their votes were cast as intended.

[11] In addition to Norway, Estonia and several Swiss cantons are introducing E2E verification mechanisms.

regulations such as the European Citizens Initiative regulatory framework[12] as well as in national regulations on e-voting as shown by the latest modification of the Swiss federal regulation on e-voting.

B. Updating policy

Experiences indicate that an update of the Recommendation is currently necessary to reflect lessons learned and new developments. Additionally, a management and maintenance policy for the Recommendation is needed. This is necessary in particular if the Recommendation is conceived as a check-list of requirements with respect to technical requirements that embed legal principles for democratic elections. Experts from different disciplines such as law, engineering, mathematics etc. must be involved in the maintenance work. Their proposals should be validated by member States' representatives before being presented to the Committee of Ministers with the request to formally update the Recommendation.

In this respect it is necessary to define an updating policy and the scope and purpose of updates. An updating opportunity cannot be used to question everything continually. An update being a further development of issues, it is up to the body responsible for mandating the update also to define and scope it.

Update rates can fit in the biennial review cycle of Rec(2004)11 which is meant for recommendations and updates to be discussed in detail. However, the bulk of the work needs to be conducted by experts who will most probably meet more frequently, physically or virtually, in between meetings. Work done by them must be presented to and validated by member States' representatives at biennial meetings.

Biennial review meetings are important and fulfil their mandate as long as they have an active role in the updating of the Recommendation. If no update is proposed, if there is no follow-up on countries' experiences and lessons learned, the Recommendation will gradually become obsolete and biennial meetings would lose their substance.

C. Final remarks

E-voting regulations are still in their infancy and have not yet reached the maturity of the rest of electoral legislation. This is also true for Rec(2004)11 whose application in the past ten years provides us with important lessons which, in return, call for an update.

If work in 2004 started from a theoretical perspective, updating work in 2014 should start by considering the practical needs of administrations, voters, industry and other stakeholders.

The initial enthusiasm for e-voting in 2004 has given way to more lucidity and maturity in the consideration of risks and opportunities. Today's understanding of IT and e-voting should be duly taken into account in the updating process.

The aim is to ensure that the Recommendation is up-to-date, balanced and responsive to ongoing developments. A revised Recommendation would allow the Council of Europe to maintain its position as a recognised and cutting-edge actor in the field of e-voting.

[12] See Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative, (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:065:0001:0022:en:PDF) and the Commissions' implementing regulation of 17 November 2011 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:301:0003:0009:EN:PDF)

All internet sources cited in this paper were accessed end August 2014

[1] Barrat, J. and Goldsmith, B. (2012) *Compliance with International Standards, Norwegian e-vote project*, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic7_Assessment.pdf

[2] Barrat, J., Goldsmith, B. and Turner, J. (2012) *International Experience with Internet Voting, Norwegian e-vote project*, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf

[3] Barrat, J., Goldsmith, B. and Turner, J. (2012) *Speed and Efficiency of the Vote Counting Process, Norwegian e-vote project*, http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic4_Assessment.pdf

[4] Barrat, J., Chevallier, M., Goldsmith, B., Jandura, D., Turner, J. and Sharma, R. (2012) "Internet voting and individual verifiability: the Norwegian return codes", in Kripp, M., Volkamer, M., Grimm, R. (Eds.) *Electronic Voting 2012, Proceedings of the 5th Conference on Electronic Voting 2012 (EVOTE2012)*

[5] Barrat, J. (2012) *Observing e-enabled elections: how to implement regional electoral standards*, http://www.idea.int/democracydialog/upload/Observing-e-enabled-elections-how-to-implement-regional-electoral-standards.pdf

[6] BeVoting, (2007) *Study of electronic voting systems, Part I, 15 April 2007 and Part II, 12 October 2007*, Part I http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf, Part II http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections2011/fr/presentation/bevoting-2_gb.pdf

[7] Braun, N. (2004) 'E-Voting: Switzerland's Projects and their Legal Framework – in a European Context' in Prosser, A. and Krimmer, R. (Eds.) *Electronic Voting in Europe. Technology, Law, Politics and Society*, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), Volume P-47, pp. 43-52.

[8] Bundesverfassungsgericht (2009), Decision *2 BvC 3/07, 2 BvC 4/07, of 3 March 2009*, http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.htm

[9] CALTECH/MIT Voting Technology Project (2012) *Voting, What has changes, What hasn't & What needs improvement* http://vote.caltech.edu/content/voting-what-has-changed-what-hasnt-what-needs-improvement

[10] (The) Carter Center (2012) *The Carter Center Handbook on observing electronic voting, second edition*, http://www.cartercenter.org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook.pdf

[11] Commission des lois constitutionnelles du Sénat français/Anziani, A. and Lefèvre A. (2014) *Rapport d'information no 445 (2013-2014) sur le vote électronique*, http://www.senat.fr/rap/r13-445/r13-445.html

[12] Commission Nationale de l'Informatique et des Libertés/France (CNIL) (2010), *Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique*, http://www.cnil.fr/documentation/deliberations/deliberation/delib/249/

[13] Conseil fédéral/Suisse (2013) *Rapport du Conseil fédéral sur le vote électronique. Evaluation de la mise en place du vote électronique (2006-*

2012) et bases de dévelopment, du 14 juin 2013, http://www.bk.admin.ch/themen/pore/evoting/07977/index.html?lang=fr

[14] Council of Europe (2011) *Certification of e-voting systems, Guidelines for developing processes that confirm compliance with prescribed requirements and standards*, http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf.

[15] Council of Europe (2011) *Guidelines on transparency of e-enabled elections*, http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf

[16] Council of Europe/Susanne Caarls (2010) *E-voting handbook, Key steps in the implementation of e-enabled elections*, http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting2010/Biennial_Nov_meeting/ID10322 GBR 6948 Evoting handbook A5 HD.pdf

[17] Council of Europe (2004) *Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, adopted by the Committee of Ministers on 30 September 2004, https://wcd.coe.int/ViewDoc.jsp?id=778189

[18] Council of Europe (2004) *Explanatory Memorandum to the Draft Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, https://wcd.coe.int/ViewDoc.jsp?id=778189

[19] Driza Maurer, A. (2013) *Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 29 November 2013*, http://www.electoralpractice.ch/wp-content/uploads/2014/01/REPORT-DRIZA-MAURER-20131129.pdf

[20] Ehringfeld, A., Naber, L., Grechenig, T., Krimmer, R., Traxl, M. and Fischer, G. (2010) "Analysis of Recommendation Rec(2004)11 based on the experiences of specific attacks against the first legally binding implementation of e-voting in Austria", in Krimmer, R. and Grimm, R. (Eds.) *Electronic Voting 2010 (EVOTE10)*, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), Volume P-167, pp. 225-237

[21] Electronic Frontier Finland, Vähä-Sipilä, A. (ed.) (2009) *A report on the finish e-voting pilot*, http://www.effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf

[22] European Commission for Democracy through Law (Venice Commission)/Grabenwarter, Ch. (2004) *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe*, http://www.venice.coe.int/webforms/documents/CDL-AD(2004)012.aspx

[23] European Commission (2006) *Methodological Guide on Electoral Assistance*, http://ec.europa.eu/europeaid/multimedia/publications/documents/thematic/ec_methodological_guide_on_electoral_assistance_en.pdf

[24] Goldsmith, B. (2011) *Electronic Voting & Counting Technologies, A Guide to Conducting Feasibility Studies*, IFES Election Technology Series, http://www.ifes.org/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf

[25] IDEA (2011) *Introducing electronic voting, Essential Considerations. Policy paper*, http://www.idea.int/publications/introducing-electronic-voting/

[26] Jones, D. (2004) *The European 2004 Draft E-Voting Standard: Some critical comments*, http://homepage.cs.uiowa.edu/~jones/voting/coe2004.shtml

[27] Krimmer, R. (2012) "The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy", *Tallinn University of Technology Doctoral Theses Series I: Social Sciences, No. 19*

[28] Loeber, L. (2008) "E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years" in Krimmer, R. and Grimm, R. (Eds.) (2008) *Electronic Voting 2008 (EVOTE08)*, Lecture Notes in Informatics (LNI) - Proceedings Series of the Gesellschaft für Informatik (GI), Volume P-131

[29] Madise, Ü. and Vinkel, P. (2011) "Constitutionality of Remote Internet Voting: The Estonian Perspective", *Juridica International. Iuridicum Foundation*, Vol. 18, pp. 4–16.

[30] McGaley, M. and Gibson, J.P. (2006) *A Critical Analysis of the Council of Europe Recommendations on e-voting*, https://www.usenix.org/legacy/event/evt06/tech/full_papers/mcgaley/mcgaley.pdf

[31] Norway (2013) *Regulations relating to trial internet voting during advance voting and use of electronic electoral rolls at polling stations on election day during the 2013 parliamentary election in selected municipalities*, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_relating_to_trial_internet_voting_2013.pdf

[32] Norway (2011) *Regulations relating to trial electronic voting during advance voting, use of electoral roll at polling stationsand use of new ballot papers at the 2011 municipal and county council elections in the selected municipalities of Bodø, Bremanger, Hammerfest, Mandal, Radøy, Re, Sandnes, Tynset, Vefsn and Ålesund, and the county municipalities of Møre og Romsdal, Hedmark, Vestfold, Vest-Agder, Rogaland, Hordaland, Sogn og Fjordane, Nordland and Finnmark*, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/E-valgsforskriften_endelig_versj_230611_engelsk.pdf

[33] Organisation of American States (2010) *Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions*, http://www.oas.org/es/sap/docs/Technology English-FINAL-4-27-10.pdf

[34] OSCE/ODIHR (2013) *Handbook for the observation of new voting technologies*, http://www.osce.org/odihr/elections/104939

[35] Pran, V. and Merloe, P. (2008) *Monitoring electronic technologies in electoral processes: an NDI guide for political parties and civic organizations*, http://www.ndi.org/node/14616

[36] Presidential Commission on Election Administration (2014) *The american voting experience: Report and Recommendations of the Presidential Commission on Election Administration*, https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf

[37] Remmert, M. (2004) "Towards European Standards on Electronic Voting", in Prosser, A. and Krimmer, R. (Eds.), *Electronic Voting in Europe - Technology, Law, Politics and Society*, P-47, Gesellschaft für Informatik, pp. 13–16.

[38] Republic of Estonia, Supreme Court, *Judgment of the Constitutional Review Chamber of the Supreme Court, Decision 3-4-1-13-05, 1st September 2005*, http://www.nc.ee/?id=381

[39] Schwartz, B. and Grice, D. (2013) *Establishing a legal framework for e-voting in Canada*, http://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf

[40] U.S. Election Assistance Commission (EAC) (2011) *A survey of Internet Voting*, http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf

[41] U.S. Election Assistance Commission (EAC) (2005) *2005 Voluntary Voting System Guidelines*, http://www.eac.gov/testing_and_certification/2005_vvsg.aspx

[42] Verfassungsgerichtshof (2011) Decision *V 85-96/11-15, 13 December 2011*, http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/6/7/CH0006/CMS1327398738575/e-voting_v85-11.pdf

[43] Volkamer, M. (2009) *Evaluation of Electronic Voting, Requirements and Evaluation Procedures to Support Responsible Election Authorities*, Springer-Verlag Berlin Heidelberg 2009

[44] Whitmore K., Congress of Local and Regional Authorities (2008) *Information Report on the Electronic Voting in the Finnish Municipal Elections observed on 26 October 2008, 1 December 2008*, https://wcd.coe.int/ViewDoc.jsp?id=1380337&Site=Congress

[45] Yard, M. (Ed.) (2010) *Direct Democracy: Progress and Pitfalls of Election Technology*, IFES Election Technology Series, http://www.ifes.org/Content/Publications/Books/2010/Direct-Democracy-Progress-and-Pitfalls-of-Election-Technology.aspx

Electronic Voting in Polling Stations

Implementation and Evaluation of the EasyVote Tallying Component and Ballot

Jurlind Budurushi
and Melanie Volkamer
Computer Science Department
Technische Universtität Darmstadt
Darmstadt, Germany
Email: name.surname@cased.de

Karen Renaud
School of Computing Science
University of Glasgow, UK
Email: karen.renaud@glasgow.ac.uk

Marcel Woide
Psychology Department
Technische Universtität Darmstadt
Darmstadt, Germany
Email: marcel.woide@cased.de

***Abstract*—The German federal constitutional court ruled, in 2009, that elections had to have a public nature. EasyVote, a promising hybrid electronic voting system for conducting elections with complex voting rules and huge ballots, meets this requirement. Two assumptions need to hold, however. The first is that voters will verify the human-readable part of the EasyVote ballot and detect discrepancies. Secondly, that electoral officials will act to verify that the human-readable part of the ballot is identical to the machine-readable part, and that they, too, will detect discrepancies. The first assumption was tested in prior work, so in this paper we examine the viability of the second assumption.**

We developed an EasyVote tallying component and conducted a user study to determine whether electoral officials would detect discrepancies. The results of our user study show that our volunteer electoral officials did not detect all of the differences, which challenges the validity of the second assumption.

Based on these findings we proceeded to propose two alternative designs of the EasyVote ballot: (1) In contrast to the original EasyVote ballot, the human-readable part highlights only the voter's direct selections in orange, i.e. votes that are automatically distributed by selecting a party are not highlighted; (2) The second alternative includes only the voter's direct selections and highlights them in orange. Both alternatives reduce the number of required manual comparisons and should consequently increase the number of discrepancies detected by election officials. We evaluated both alternatives in an online survey with respect to ease of verification and understandability of the cast vote, i.e. verifying that the human-readable part contained the voter's selections and understanding the impact (distribution of votes) of the corresponding selections.

The results of the online survey show that both alternatives are significantly better than the original EasyVote ballot with respect to ease of verification and understandability. Furthermore, the first alternative is significantly better than the second with respect to understandability of the cast vote, and no significant difference was found between the alternatives with respect to ease of verification of the cast vote.

I. Introduction

The German saying "different countries, different customs" holds true for elections, which can be very different between and even within countries. Some elections, like parliamentary elections in Estonia or Germany have very simple voting rules and small ballots. Voters can select 1 out of n-candidates, where n is a relatively small number between two and 20. Other elections, like parliamentary and European elections in Luxembourg, parliamentary elections in Belgium and local elections in Germany (e.g. Bavaria, Bremen, Hamburg, Hesse), have very complex voting rules and huge ballots. In this paper we focus on the local elections in Hesse, because we were able to access original materials, e.g. ballots, tallying software and training presentations, used in the 2011 elections. In these elections voters can cast up to 93 votes[1] depending on the size of the district; usually more than ten parties and more than 450 candidates participate, which results in huge ballots, nearly the size of an A0[2] sheet of paper (Size: 27" x 35"). Furthermore, voters can select a party (votes are automatically assigned to the candidates of the selected party according to the list order), and cross out candidates they do not like. They can perform vote splitting (cast votes for candidates of different parties) and cumulative voting (cast up to three votes for each candidate). Such complexity introduces challenges regarding both vote casting and tallying processes. In the vote casting process, voters might unintentionally spoil their vote, due to the complex voting rules. Furthermore, the tallying process is very time intensive and likely to be error prone, because of the combination of complex voting rules and huge ballots.

In order to address these challenges and improve the situation for both voters and poll workers, in particular for local elections in Hesse, Volkamer *et al.* [2] proposed an electronic voting system, called EasyVote. The EasyVote system can be briefly described as follows: 1) Voters prepare their ballots on a voting device, which prints their selections. The printed ballot contains voters' selections in a human- and machine-readable (a plaintext QR-Code) format. 2) Voters deposit their ballots into the ballot box. 3) Ballots are tallied automatically, by scanning the QR-Codes on the printouts.

Budurushi *et al.* [3] evaluated a number of electronic voting systems with respect to their feasibility for use in elections with complex voting rules and huge ballots. They report that, with respect to the *public nature of elections*[3] and

[1]This number depends on the the number of available seats, which also limits the number of candidates nominated by a party.

[2]A0 according to [1].

[3]This principle was introduced by the Federal Constitutional Court of Germany in 2009, and states that it must be possible for the citizen to verify the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge, i.e. each election step must be transparent for the voter.

secrecy legal requirements, the EasyVote system supported the complex local elections in Hesse better than the other systems. Henning *et al.* [4] analysed the EasyVote system from a legal perspective and showed that it complied with German requirements for local elections in Hesse.[4] Both analyses [3], [4] rely on the following assumptions being true: (1) Voters will act to verify the correctness of the human-readable part of their ballots; (2) Voters will detect discrepancies; (3) Electoral officials will verify that the human-readable matches the machine-readable part (QR-Code); (4) Electoral officials will detect discrepancies. However, before EasyVote can be used in practice, the validity of these assumptions has to be verified. With respect to the first and second assumptions, Budurushi *et al*. [5] showed that the number of voters that verified their printouts and detected discrepancies could be increased significantly if voters were provided with pre-printed, "just-in-time" verification instructions.

Thus, in the first part of this paper we focus our attention on the actions of electoral officials during the tallying process. We implemented a tallying component prototype based on the EasyVote system. The tallying process itself could, in general, be achieved using different techniques: (1) by scanning the printouts with different scanners manufactured by different manufacturers (trust distribution), or (2) by scanning printouts and performing either risk-limiting audits described in [6] and [7], or the Bayesian method described in [8], or (3) by scanning each ballot and comparing the human-readable printout with the details on the screen (generated from the QR-Code). We implemented the latter process, as this complies with the legal requirements [4]. We do not know whether the other techniques are aligned with the public nature of elections, because, to the best of our knowledge, no legal analysis has been conducted yet. Since electoral officials have to scan a large number of individual ballots, one after the other, the accuracy of the process becomes important and therefore should be evaluated. Accuracy is particularly important, because it relies on human attention, which is notoriously unreliable [9], [10]. This is especially the case when the prevalence of the target to be noticed is low [11], [12], when the searcher has to look for multiple different targets at the same time [13] and when the size of the area to be searched is large [14]. All of these are true for the EasyVote ballots so it seems important to test the impact of this well-known human limitation on the checking required during the EasyVote tallying process. Therefore in a user study, we evaluated the *accuracy* of the EasyVote tallying component by intentionally introducing manipulated printouts, i.e. printouts where the human-readable part did not match the machine-readable part (the data stored in the QR-Code). Note that the goal was to evaluate the *accuracy* of the actions of electoral officials during the implemented tallying process, thus we assumed a compromised vote casting component and an honest and correctly implemented EasyVote tallying component. The results of this study show that this way of effecting the tallying in EasyVote is not fully accurate as we rely on human ability to detect differences and our participant "electoral officials" did not detect all the manipulations we introduced during their scanning and verification process. The study also revealed that it will be necessary either to improve the EasyVote system or to relax the legal requirements.

Based on these findings, in the second part of this paper we focused on improving the process and proposed two alternative EasyVote ballot designs: (1) In contrast to the original EasyVote ballot, the human-readable part highlights the voter's direct selections in orange, i.e. votes that are automatically distributed by selecting a party are not highlighted; (2) The second alternative includes only the voter's direct selections and highlights them in orange. Both alternatives reduce the number of required manual comparisons and should consequently increase the number of discrepancies detected by the poll workers. We evaluated the alternatives in an online survey with respect to *ease of verification* and *understandability* of the cast vote, i.e. verifying that the human-readable part contains the voter's selections and understanding the impact (distribution of votes) of the corresponding selections. The results of the online survey show that the alternatives are significantly better than the original EasyVote ballot with respect to ease of verification and understandability of the cast vote. Furthermore, the first alternative is significantly better than the second with respect to understandability of the cast vote, and no significant difference was found between the alternatives with respect to ease of verification of the cast vote.

II. Background

We first explain the traditional tallying process in the local Hesse elections. The paper ballots used in the traditional local elections in Hesse are shown and elaborated on in Figure 1. The traditional tallying process in the local elections in Hesse comprises two phases. Both phases are led by an electoral official who gives instructions to other electoral officials and observes the process. In the first phase, at the end of the election day, electoral officials perform the following steps:

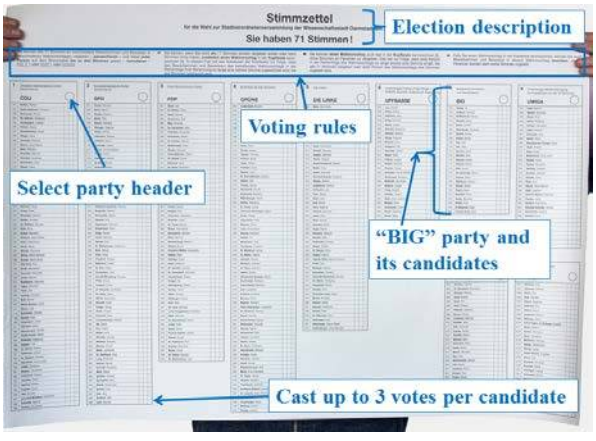


Fig. 1: Paper ballot of the local elections in Hesse in 2011. (Size: 27" x 35")

- Open the ballot boxes, count the total number of cast ballots and compare it with the total number of marked voters in the electoral register.

[4]As the legal evaluation is in German, we outline here the most important conclusions: (1) Voters can verify their vote without any specialist knowledge. (2) Voters are not required to rely on the system's integrity. (3) The system enables an automatic tally of single votes, and also a full manual tallying of votes, similar to the traditional one. (4) The human-readable part is the deciding factor regarding the tallying process. (5) The system strengthens the principle of the "public nature of elections", since on the one hand voters can better understand the impact of their selections, and on the other hand the tallying process might be faster and more accurate than the traditional one.

- Divide the ballots into four categories: 1) Only party header is marked 2) Candidates and/or a party header are marked 3) Invalid 4) Not assignable to 1), 2) or 3).
- Check that ballots are assigned to the correct category.
- Divide and count the 1st category by parties (first intermediate result).
- Discuss and assign each single ballot of the 4th to the 1st, 2nd or 3rd category.
- Manually recompute the intermediate election result, based on the 1st and 3rd category.

The second phase of the tallying process takes place the day after the election. This phase is supported electronically by special purpose software. The software used by traditional local elections in Hesse is called PC-Wahl.[5] During this phase only ballots from the 2nd category, i.e. ballots that contain marked candidates and/or a party header, are tallied. Electoral officials perform the following steps:

- Electoral officials enter the intermediate result from the first phase.
- First five ballots are entered and recorded into the PC-Wahl interface (Figure 2).
- Manually tally the first five ballots.
- Compare the electronic result with the manual result.[6]
- Enter and record the rest of the ballots into the corresponding PC-Wahl interface.
- Electronically compute the final election result, and sign the printed disposition.

The process of entering and recording ballots via the corresponding PC-Wahl interface is performed by three electoral officials. One electoral official narrates the marks from the ballot and a second enters them into the PC-Wahl interface. A third electoral official verifies that the first and second electoral officials have performed this correctly.

Note that electoral officials who participate in the second phase of the tallying process are employees of the corresponding electoral office and/or municipality. Hence, they have relatively high technical expertise. Furthermore, they participate in a theoretical training workshop regarding the PC-Wahl software. The workshop lasts approximately 30 minutes, and electoral official can practice if they wish to, in order to ensure their competence.

III. Implementation

In this section we introduce and describe the different steps of the implemented EasyVote tallying process. The EasyVote ballots that need to be tallied are shown in Figure 3. Afterwards, we present the interfaces of the implemented prototype.

[5]http://www.pcwahl.de/.

[6]This check only serves as a self-control for electoral officials, rather than checking the correctness of PC-Wahl.

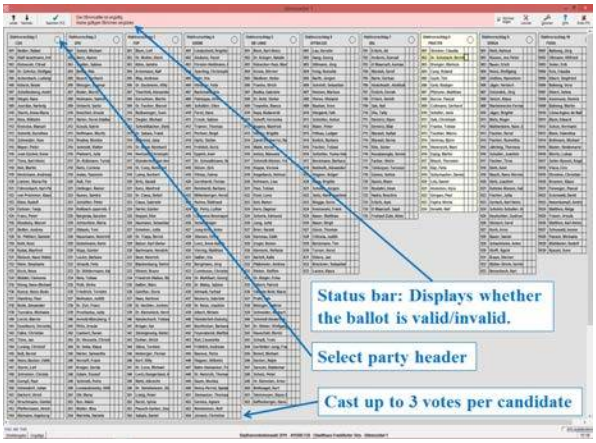


Fig. 2: Ballot entering and recording interface of PC-Wahl.

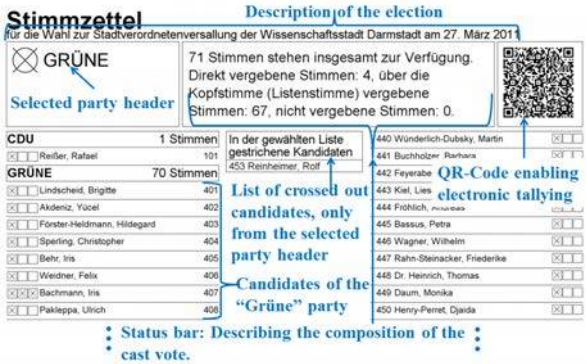


Fig. 3: The EasyVote paper ballot.

A. Tallying Process

The implemented EasyVote tallying process comprises the following steps: (1) Open the ballot boxes, count the total number of cast ballots and compare it with the total number of marked voters in the electoral register. (2) Scan each individual ballot. (3) Electronically compute the final election result, and sign the printed disposition.

Since the EasyVote ballots are electronically prepared and printed in a pre-defined layout, format and font, the ballots could feasibly be scanned by using Optical Character Recognition (OCR) scanners. However, for scanning each individual ballot we decided to use QR-Codes scanners, as originally proposed by Volkamer *et al.* [2], based on the following general advantages of QR-Code scanners:

- QR-Code scanners provide a much higher error correction level and therefore are more accurate.
- QR-Code scanners can be used for all type of ballots (universal encoding), while OCR scanners need to be configured and maintained for each type of ballot.

Hence, the process of scanning and counting an individual ballot, shown in Figure 4, consists of the following steps: (1) Pick up a ballot. (2) Scan the QR-Code. (3) Verify and confirm

that the scanned information matches the human-readable part of the ballot. (4) Repeat process with the next ballot.

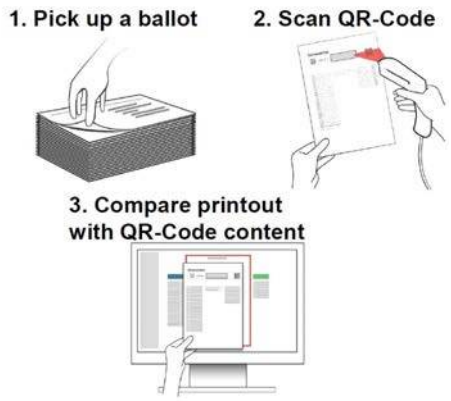


Fig. 4: Scanning and counting ballots with EasyVote.

Note that if we used OCR scanners the human-readable part is also the machine-readable part. This prevents the vote casting component from manipulating the machine-readable part, because voters would be able to detect the manipulation. However, in order to ensure the correctness of the scanning/counting process, electoral officials are still required to fully verify/examine the scanned ballot against the printout (EasyVote ballot). If we assume that electoral officials are required to detect *all* possible discrepancies, it makes no difference whether these are introduced by the vote casting or tallying components.

B. Interfaces of the Prototype

The EasyVote tallying component proposed by Volkamer *et al.* [2] uses two monitors (two different interfaces) for the tallying process. The first monitor, presented in step three on Figure 4, displays and enables the verification of each individual scanned ballot. The second monitor displays intermediate election results after scanning, verifying and confirming each individual ballot. This enables electoral officials and the general public to verify that each individual ballot is correctly added to the election result.

Figure 5 presents the implemented interface for the first monitor, while Figure 6 presents the implemented interface for the second monitor.

IV. User Study - Accuracy Evaluation

In this section we describe the user study, in which we evaluated the prototype with respect to accuracy. The goal of the study was to find out if the implemented EasyVote tallying component is 100% accurate, i.e. that discrepancies where the QR-Code does not match the human-readable part can always (in any case and by any participant) be detected. We intentionally introduced manipulated printouts, in order to check if participants detected the discrepancies.

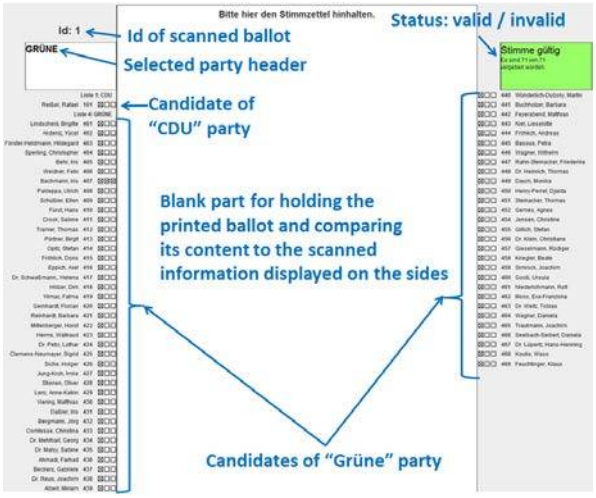


Fig. 5: Scanning and verifying the content of the current ballot.

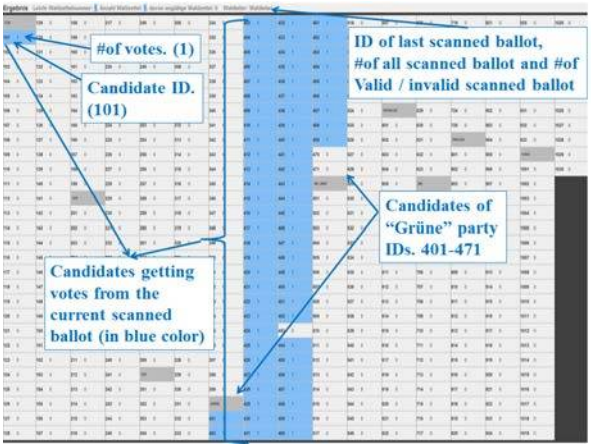


Fig. 6: Overview on the intermediate election result.

A. Preliminary Considerations and Materials

In the user study we only focused on the process of scanning an individual ballot and verifying that the human-readable part matches the machine-readable part. Although by verifying intermediate results we might also be able to detect discrepancies, we assume that if participants cannot detect all discrepancies during the scanning and verifying process, they will also not detect further discrepancies while verifying intermediate results. Thus, for this study we assumed a compromised vote casting component and, an honest and correctly implemented EasyVote tallying component. Note that in practice the tallying component is not assumed trustworthy, as different mechanisms can be used to detect a malicious tallying component, for instance the tallying component provides a cryptographic commitment after each scanned ballot or a hash chain, or by videotaping both monitors at the same time. Afterwards, random checks can be performed to ensure the correctness of the election result.

Furthermore, one of the most well-known challenges in the area of usable security is that you cannot communicate

the primary goal of the study to participants without biasing them [15]. If participants know the primary goal of the study, they may act in a manner perceived as appropriate, and change their behaviour [16]. Therefore we told all participants in the user study that the goal was to evaluate the usability of the EasyVote tallying component. This was necessary so that the participants would not be biased in their behaviour.

The materials required to conduct the user study are listed here. For the materials from the local elections in Hesse we collaborated with the local authorities.

- Training workshop presentations for the PC-Wahl software.
- 189 original electronically filled in ballots from the local elections in Hesse 2011. They were split as follows: 94 from the 1st, 89 from the 2nd and 6 from the 3rd category.[7]
- The implemented EasyVote tallying component.
- Training workshop presentations for the EasyVote system. We created these presentations based on those for the PC-Wahl software.
- 189 EasyVote ballots. These ballots were electronically created, and duplicated the 189 traditional ballots.
- Five EasyVote test ballots to be used during the training phase: Three ballots with candidates and party header marked, and two ballots that also contained crossed out candidates. Two of the five ballots required corresponding corrections by the participants.

B. Study Design

In order to evaluate the accuracy of the implemented EasyVote tallying component we manipulated the QR-Codes of the EasyVote ballots. Hence, when scanning the QR-Code of a manipulated ballot participants should detect a discrepancy between the EasyVote ballot and the data displayed on the screen. As we do not aim to change, but rather to improve the tallying process for local elections in Hesse, participants were required to tally only ballots of the 2nd category, i.e. a total of 89 ballots that contain votes assigned to candidates and/or a selected party header.

C. Manipulations: Introducing Discrepancies

While manipulating the QR-Codes of the EasyVote ballots is technically trivial, we first had to solve the following challenges: 1) Identify all possible manipulations that lead to a difference between the printed human-readable part on the ballot and the data displayed on the monitor; 2) Select an adequate set of manipulations; 3) Introduce an adequate number of manipulations, in order to not directly reveal the study goal; 4) Decide how to randomly add manipulations to ballots; 5) Decide how to introduce the manipulations into the ballot set randomly.

By performing a systematic analysis we identified 36 possible manipulations that we classified in the following five manipulation categories: 1) Changing only vote distribution (7 manipulations); 2) Change candidate names (14 manipulations); 3) Changing party, including its candidates (11 manipulations); 4) Invalidating a valid ballot (2 manipulations); 5) Validating an invalid ballot (1 manipulation).

In order to select a reasonable set of manipulations, we defined the following criteria: 1) Detecting the manipulation requires a full and careful comparison of the EasyVote ballot and monitor; 2) Manipulation should be hard to detect. This led us to the following adequate manipulation set:

- Remove votes from a candidate and assign them to another candidate (1st manipulation category).
- Remove votes from a candidate and do not re-assign them (1st manipulation category).
- Remove a candidate and insert another candidate instead (2nd manipulation category).
- Remove a candidate (2nd manipulation category).
- Remove a party, including its candidates (3rd manipulation category)

This set also covers the manipulations used in previous studies, refer to [17] and [18].

Furthermore, since we were restricted by the number of ballots used in this study we manipulated only 5 out of the 89 ballots. In this way we covered all manipulation categories and introduced a reasonable number of manipulations relative to the number of ballots, such that participants would not guess the primary study goal. We randomly selected 5 ballots and introduced the manipulations according to a random permutation. Finally, we randomly introduced the manipulated ballots into the set of all ballots. Note that each group was confronted with the same manipulations, but in a different random order.

D. Experimental Design and Procedure

11 participants were randomly allocated to four different groups. Three groups consisted of three participants, and one group of two. Each group had to perform the following steps:

- Read and sign the agreement form for participating to the study.
- Participate in the training workshop.
- Tally the 2nd category ballots with the implemented prototype.
- Debrief.

Furthermore, we randomly assigned participants of a group the following tasks: 1) Scanning (one participant had to scan the ballot); 2) Verifying (two participants had to verify that the human-readable part matches the machine-readable part). As the last group consisted only of two participants, one of the participants was randomly assigned to perform both tasks.

Note that the EasyVote tallying process proposed by Volkamer *et al.* [2] requires only two electoral officials. However, we used the same setting as in the traditional local elections in Hesse, thus assigning three instead of two participants (electoral officials) to each group. The last group consisted

[7] Refer to section II for the description of the different categories.

only of two participants, because one of them did not show up.

E. Experimental Setup and Ethical Considerations

All experiments took place in our department. The venue was equipped with tables, chairs and a projector. The projector was used during the presentations in the training workshops. All groups were provided with the necessary hardware equipment, monitor(s), a computer on which the tallying software was installed, and a printer.

An ethics commission at our university provides ethical requirements for research involving humans. These requirements were met. All participants were told that all data would be stored anonymously and used only for the purposes of the experiment.

F. Recruiting and Sampling

The participants were recruited via e-mail, advertising in social networks and flyers. The experiment had 11 randomly selected participants (6 female, 5 male), age 19-57 years: 7 students from different subject areas and 4 employees of our university. All participants were naïve, with respect to the content, since none had worked as an electoral official before. Three different incentives encouraged participation: First, the employees of our university were interested in science and wanted to support our research. Second, 3 were psychology students, who are required by their department to participate in 30 hours of research studies. We compensated them with the appropriate amount of hours. For the rest of the participants we provided €10 per participant.

It is important to note that most of the participants were university students who are very familiar with technology. While they may not be representative of the larger "electoral officials" population, they probably serve a best-case scenario for what tallying performance could be.

G. Results

In this section we report the results regarding the dependent variable "detected" that reflects the accuracy of the implemented EasyVote tallying component. Table I summarises the results of the study. "True" means that the discrepancy was detected and corrected by the participants, while "False" means that the discrepancy was not detected.

TABLE I: Summary of the accuracy evaluation.

Manipulation categories*	Group 1 / Position	Group 2 / Position	Group 3 / Position	Group 4** / Position
1	False / 1	True / 34	True / 6	True / 59
2	True / 83	False / 75	True / 68	True / 8
3	True / 51	False / 36	True / 88	False / 89
4	False / 9	True / 67	True / 25	False / 3
5	True / 87	True / 46	False / 54	True / 36

* Refer to section II for the description of the different categories.
** This group consisted only of two participants.

The results of the accuracy evaluation show that none of the groups detected all introduced discrepancies. Furthermore, the results indicate that detecting a discrepancy does not depend on the position, or on whether others have previously been detected, or on the specific manipulation category.

Note that due to these results, which already show that the implemented EasyVote tallying component does not achieve 100% accuracy, we decided not to continue the user study, i.e. not to include further groups (participants) enabling us to achieve an adequate sample size that would allow to perform various statistical tests.

V. Online Survey - EasyVote Ballot Design

In this section we describe our online survey and present the results. This survey is motivated by the results of the user study reported in the first part of the paper. Hence, the goal was to identify an alternative EasyVote ballot design. On the one hand it ought to reduce the number of required manual comparisons and consequently increase the number of discrepancies detected by poll workers. On the other hand it enables voters easily to verify their cast vote. We also report on recruitment and sampling of participants.

A. Alternative EasyVote Ballots

In the survey we presented participants with two possible EasyVote ballot designs (see Figure 7). In contrast to the original EasyVote ballot, both alternatives introduce colour as a new dimension. According to Braun and Silver [19], the colour red conveys the highest level of perceived hazard followed by orange, black, green and blue. Furthermore, Young and Wogalter [20] found that with respect to memory times print highlighted with orange was better remembered than non-highlighted text. Moreover, since red is problematic for a significant percentage of the male population due to colour blindness, orange seemed the best choice.

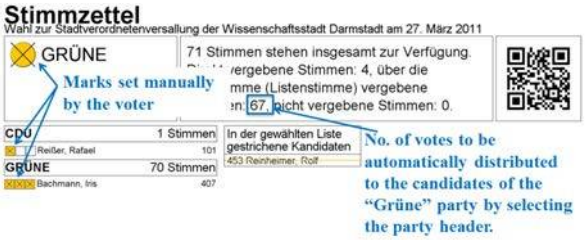
The first alternative, in contrast to the original EasyVote ballot, highlights the voter's manual selections in orange. The second alternative simplifies things even further, since it eliminates everything except the voter's manual selections and these are still highlighted in orange. Hence, automatically distributed votes, i.e. remaining votes that are assigned to the candidates of a party by selecting the party header, are not printed. The size of the printout remains the same, independent of the voter's selections.

Furthermore, in contrast to the original EasyVote ballot, the machine-readable part (QR-Code) encodes only the voter's manual selections. Thus, the "adapted" EasyVote tallying component implements the algorithm to automatically distribute votes independently of the voter's manual selections, rather than only relying on the data stored in the QR-Code. Both alternatives reduce the number of required manual comparisons for both voters and electoral officials. However, in order to ensure the correctness of the election result, we suggest that electoral officials check the automatic distribution of votes for a random set of ballots, i.e. verify the complete ballot displayed/interpreted by the tallying component, rather than only voter's manual selections.

B. Design and Procedure

The survey consisted of four parts and was structured as follows: (1) Participants were introduced to the local elections

(a) The first alternative.



(b) The second alternative.

Fig. 7: The alternative EasyVote ballot designs

in Hesse. They were asked whether they had previously cast a vote in local Hesse or similar elections, and how often they participated in local elections. (2) Participants were told how many invalid votes were cast in the local elections in Hesse in 2011. This percentage, (5.5%)[8] was much higher than the German federal elections in 2013 (on avarage 2.7%)[9]. Then they were introduced to the EasyVote vote casting process. (3) They were asked some general questions to assess the comprehensibility of the EasyVote vote casting process. (4) Participants were given a textual description of a cast vote, and confronted with the original and the two alternative ballots. All reflected the cast vote described in the text. Participants were asked to rank the ballot types (original and alternatives) with respect to ease of verification and understandability of the cast vote, i.e. verifying that the human-readable part contains the voters selections and understanding the impact (distribution of votes) of the corresponding selections. We also collected some demographic data (nationality, age, gender and education).

C. Recruiting and Sampling

The participants were recruited via e-mail, advertising in social networks, flyers and by personal contact. 87 subjects participated (35 female, 48 male, 4 others) between the ages of 19-75 years. We removed 14 participants (3 female, 9 male, 2 others) aged 22-75, because they did not answer all questions with respect to the vote casting process with the EasyVote voting system. The remaining 73 subjects (32 female, 39 male, 2 others) aged 19-65 comprised one participant with apprenticeship, four with a Ph.D. degree, five with middle school qualification, seven with a B.Sc. degree, seven with a technical college qualification, eight with a vocational education, 15 with a Diploma/M.Sc. degree and 26 with a high school qualification. Most (63) were Germans, four were Austrians, 2 were Turkish, one Swiss and one did not provide information about nationality. No incentives were provided, thus participation was purely voluntary.

[8]http://www.statistik-hessen.de/K2011/EK1.htm, last accessed 10.08.2014 (in German).

[9]http://www.bundeswahlleiter.de/en/bundestagswahlen/BTW_BUND_13/ergebnisse/landesergebnisse/l06/, last accessed 10.08.2014.

D. Results

Table II summarises the results with respect to understandability of cast vote and Table III with respect to ease of verification.

TABLE II: Understandability of cast vote.

	Times of ranking		
EasyVote Ballot	**First place**	**Second place**	**Third place**
Original	5	27	41
First alternative	41	30	2
Second alternative	27	16	30

TABLE III: Ease of verification of cast vote.

	Times of ranking		
EasyVote Ballot	**First place**	**Second place**	**Third place**
Original	6	18	49
First alternative	32	40	1
Second alternative	35	15	24

In order to measure the difference between the original and the alternative designs of the EasyVote ballot we used the Wilcoxon non-parametric test. The test shows a significant difference between the first alternative and the original EasyVote ballot with respect to understandability, Z=-6.722; $p < 0.01$ and ease of verification, Z=-6.722; $p < 0.01$. A significant difference is also found between the second alternative and the original EasyVote ballot with respect to understandability, Z=-2.891; $p < 0.01$ and ease of verification, Z=-4.205; $p < 0.01$. Additionally, the first and second alternatives differ significantly regarding understandability, Z=-3.673; $p < 0.01$ with a higher rank sum for the first alternative (1993.50). No significant difference was found between both alternatives regarding ease of verification.

Furthermore, we evaluated participants' statements, on a five-point Likert scale, concerning the advantages of the EasyVote system compared to the traditional elections in Hesse. Approximately 92% of the participants agreed or fully agreed that the EasyVote system would support voters in such complex elections, such as the local elections in Hesse. 64% of the participants would be happy to use the EasyVote system at the next local elections in Hesse. Around 80% of the participants recognised or fully recognised the advantages of the EasyVote system compared to traditional local elections in Hesse, and think that the EasyVote system is a first step in the right direction to introduce technology in the context of legally-binding elections. Only one participant did not perceive any advantages with respect to using the EasyVote system.

VI. Conclusion and Future Work

The focus of our research is on electronic voting systems for elections with complex voting rules and huge ballots that

meet the German constitutional requirements, including the principle of the public nature of elections. This principle requires that voters should be able to verify all essential steps of the election without technical knowledge. Therefore, in this paper we considered the EasyVote [2] hybrid voting system, which is supposed to meet those requirements. Because of the public nature of elections, we focused on the tallying process in which ballots are scanned individually and each ballot is verified as correct before being tallied.

In the first part of this paper, we reported the results of a user study carried out to evaluate the accuracy of the implemented EasyVote tallying process. The main finding is that the implemented tallying process cannot guarantee a 100% accurate election result since participants did not notice all manipulations. Such human errors could be avoided by automatically scanning all EasyVote ballots, i.e. implementing a different tallying process. Furthermore, trust could be increased either by risk-limiting audit techniques or by using several independent scanners/tallying components. However, this would decrease the extent to which the public nature principle is implemented. This result shows that just because a voting system meets the public nature requirement it does not mean that discrepancies are detected or that underlying fraud is necessarily revealed.

In the second part we reported the results of an online survey, which evaluated two alternative EasyVote ballots designs. Both alternatives were shown to reduce the number of manual comparisons required and can be expected to increase the number of discrepancies detected by the election officials. The results of the online survey show that the first alternative design, where voters' manual selections are additionally highlighted in orange, differs significantly with the original EasyVote ballot with respect to understandability and ease of verification of the cast vote. Furthermore, the first and second alternatives differ significantly regarding understandability. No significant difference was found between the alternatives with respect to ease of verification.

Thus, for future interdisciplinary research we will study the reliability of mechanisms which comply with the principle of the public nature of elections. We plan to repeat the user study with the new EasyVote ballot design (first alternative), and also to propose different techniques to improve detection accuracy. Another open research question is to discover what an acceptable rate of errors is, if indeed we have to accept that some errors will remain undetected.

ACKNOWLEDGMENT

This paper has been developed within the project 'VerkonWa' - Verfassungskonforme Umsetzung von elektronischen Wahlen - which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation). We would like to thank Paul Gerber for helpful comments and suggestions.

REFERENCES

[1] International Organization For Standardization, *ISO 216:2007: Writing paper and certain classes of printed matter – Trimmed sizes – A and B series, and indication of machine direction*. ISO, 2007.

[2] M. Volkamer, J. Budurushi, and D. Demirel, "Vote casting device with VV-SV-PAT for elections with complicated ballot papers," in *International Workshop on Requirements Engineering for Electronic Voting Systems*. Proceedings of the IEEE, 2011, pp. 1–8.

[3] J. Budurushi and M. Volkamer, "Feasibility analysis of various electronic voting systems for complex elections," in *International Conference for E-Democracy and Open Government 2014*, May 2014.

[4] M. Henning, M. Volkamer, and J. Budurushi, "Elektronische Kandidatenauswahl und automatisierte Stimmermittlung am Beispiel hessischer Kommunalwahlen," *Die Öffentliche Verwaltung (DÖV)*, no. 20, October 2012.

[5] J. Budurushi, M. Woide, and M. Volkamer, "Introducing precautionary behavior by temporal diversion of voter attention from casting to verifying their vote," in *Workshop on Usable Security (USEC)*, Feb. 2014.

[6] M. Lindeman and P. B. Stark, "A gentle introduction to risk-limiting audits," *IEEE Security and Privacy*, vol. 10, no. 5, p. 42, 2012.

[7] M. Lindeman, P. S. B, and V. Yates, "Bravo: Ballot-polling risk-limiting audits to verify outcomes," in *Electronic Voting Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*. Bellevue, WA: USENIX, 6-7 August 2012.

[8] R. Rivest and E. Shen, "A Bayesian method for auditing elections," in *Proceedings of the 2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'12)*. Bellevue, WA: USENIX, 6-7 August 2012.

[9] D. J. Madden and S. R. Mitroff, "Aging and top-down attentional control in visual search," 2010, institute for Homeland Security Solutions Research Brief. https://www.ihssnc.org.

[10] J. M. Wolfe, T. S. Horowitz, and N. M. Kenner, "Cognitive psychology: Rare items often missed in visual searches," *Nature*, vol. 435, no. 7041, p. 439440, 2005.

[11] A. N. Rich, M. A. Kunar, M. J. Van Wert, B. Hidalgo-Sotelo, T. S. Horowitz, and J. M. Wolfe, "Why do we miss rare targets? Exploring the boundaries of the low prevalence effect," *Journal of Vision*, vol. 8, no. 15, p. 15, 2008.

[12] J. M. Wolfe, T. S. Horowitz, M. J. Van Wert, N. M. Kenner, S. S. Place, and N. Kibbi, "Low target prevalence is a stubborn source of errors in visual search tasks." *Journal of Experimental Psychology: General*, vol. 136, no. 4, p. 623, 2007.

[13] T. Menneer, K. R. Cave, and N. Donnelly, "The cost of search for multiple targets: Effects of practice and target similarity," *Journal of Experimental Psychology: Applied*, vol. 15, no. 2, pp. 125–139, 2009.

[14] B. Zenger and M. Fahle, "Missed targets are more frequent than false alarms: A model for error rates in visual search." *Journal of Experimental Psychology: Human Perception and Performance*, vol. 23, no. 6, p. 1783, 1997.

[15] C. Kuo, A. Perrig, and J. Walker, "Designing an evaluation method for security user interfaces: lessons from studying secure wireless network configuration," *Interactions*, no. 3, pp. 28–31, 2006.

[16] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, "'I did it because I trusted you': Challenges with the study environment biasing participant behaviours," in *SOUPS Usable Security Experiment Reports (USER) Workshop*, Microsoft in Redmond, WA, July 14-16 2010.

[17] S. P. Everett, *The usability of electronic voting machines and how votes can be changed without detection*, Std., 2007, doctoral dissertation, Rice University, Houston, TX.

[18] B. A. Campbell and M. D. Byrne, "Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability," in *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*, ser. EVT/WOTE'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 1–1. [Online]. Available: http://dl.acm.org/citation.cfm?id=1855491.1855492

[19] C. C. Braun and N. C. Silver, "Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance," *Ergonomics*, vol. 38, no. 11, pp. 2207–2220, 1995.

[20] S. L. Young and M. S. Wogalter, "Comprehension and memory of instruction manual warnings: Conspicuous print and pictorial icons," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 32, no. 6, pp. 637–649, 1990.

Pressing the button for European elections

Verifiable e-voting and public attitudes toward internet voting in Greece

Alex Delis[†], Konstantina Gavatha[‡], Aggelos Kiayias[†], Charalampos Koutalakis[‡], Elias Nikolakopoulos[‡], Lampros Paschos[‡], Mema Rousopoulou[†], Georgios Sotirellis[‡], Panos Stathopoulos[‡], Pavlos Vasilopoulos[†]*, Thomas Zacharias[†], Bingsheng Zhang[†]

[†]Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Athens, Greece
[‡]Department of Political Science and Public Administration, National and Kapodistrian University of Athens, Athens, Greece
*CEVIPOF, SciencesPo, Paris, France
www.demos-voting.org

***Abstract*— We present the initial set of findings from a pilot experiment that used an Internet-based end-to-end verifiable e-voting system and was held during the European Elections 2014 in Athens, Greece. During the experiment, which took place on May 25th 2014, 747 people voted with our system in special voting stations that were placed outside two main polling places in Athens, Greece. The election mimicked the actual election that was taking place which included a great number of parties. After casting their ballot, voters were invited to complete online a post-election questionnaire that probed their attitudes towards e-voting. In total, 648 questionnaires were collected. We present a description of the experiment and a regression analysis of our results. Our results suggest that acceptance of the e-voting system was particularly high especially among the most educated, the technologically adept but also –somewhat surprisingly– older generations.**

Keywords—e-voting; public opinion; Greece

I. INTRODUCTION

One of the most significant challenges in the development of electronic voting is its acceptance by voters. Issues of public trust and support are often at the center of the debate on the adaptation or rejection of electronic voting systems, regardless of their technical characteristics. Even though the issue of electronic voting has attracted increased scholarly attention during the last decade, studies over the acceptance of such as system by the mass public and the factors behind individual-level variance in acceptance remain scarce. In this paper, we aim to advance the relevant literature by presenting individual-level correlates of attitudes toward electronic voting from Greece. Greece is an ideal case for testing attitudes toward e-voting in environments with low familiarity with internet use, as the country ranks quite low in internet penetration. What is more, using Greece as an example adds to the literature by evaluating attitudes toward electronic voting in Europe where such research remains very scarce, with the notable exception of [1]. In particular, this paper investigates the impact of socio-demographic and familiarity with technology on three key components of acceptance of an e-voting system, namely: a) the perceived easiness of the e-voting system b) participants' willingness to see the system being adopted for national elections and c) participants' attitudes to cast their vote remotely using an e-voting system. The trial was conducted in polling stations during the 2014 European Elections. These elections are held every four years across all EU members for the election of the European parliament. The test was not binding for participants: Upon their exit from the polling booth, electors were asked to vote again through an e-voting system should they agreed to do so. Our results suggest that acceptance of the e-voting system was particularly high especially among the most educated, the technologically adept but also –somewhat surprisingly– older generations.

II. E-VOTING EVALUATIONS

Available evidence on the public reception of an electronic voting system mainly come from the United States and Latin America (but see [1] for an application in Europe): Past research has shown that e-voting systems are viewed rather favorably by citizens who participate in the trials [2, 3]. As for individual level-factors, Sherman et al. [3] investigated the impact of a number of characteristics for the case of the US in a convenience sample consisting of 105 volunteers who replied on advertisements. Their results illustrate that acceptance of the electronic voting system depends significantly on the extent to which participants had a basic understanding of the e-voting system. On the other hand, Alvarez et al. [2] studied acceptance of different e-voting devices in the case of Colombia using a non-representative yet extended sample consisting of 2294 respondents coming from three cities. Their results showed that acceptance of the system was particularly high, exceeding 80 percent of positive responses in perceived reliability of the system and 90 percent in perceived easiness. Nonetheless, according to their findingshighly educated and –surprisingly- the eldest age groups were more likely to regard the system as more reliable.

III. PRESENTATION OF E-VOTING SYSTEM DEMOS

Demos is a remote e-voting system that supports end-to-end verifiability (i.e. the voter verifies that her vote was tallied properly) and voter privacy. The system employs code-voting as introduced by Chaum [4] with a number of

modifications both in terms of usability as well as in terms of verifiability. In code-voting based systems, the voters obtain a ballot that contains a list of the candidates, each of them associated with a unique vote-code, and vote by submitting the vote-code that corresponds to the candidate of their choice. Tallying takes place by combining cryptographic elements that relate to the submitted vote-codes. The system utilizes a number of cryptographic elements that include *perfectly binding commitments* and suitably designed *zero-knowledge (ZK) proofs*.

For brevity we do not present here all the cryptographic details of Demos, which are independent of our experiment. The front-end of Demos, which is the most relevant to our experiment and explained in detail below, could have been fitted with any other code-voting system in the back-end and provide the same voting experience.

A. Setup

In the pre-election phase, an *election authority* (EA) generates ballots that have a unique serial number and consist of two equivalent parts (**A** and **B**) containing all information needed to vote. Namely, in each part, every candidate is associated with a randomly generated vote-code, which is cryptographically paired with a *vote-code recording receipt* (Fig. 1). This ballot format is called a *double ballot*. The double ballots are randomly distributed to the voters by EA or another distribution authority. Next, the EA uses the commitment scheme to create a table **T** where all ballot information is committed via the perfectly binding commitments (the candidates are first encoded and then committed). The committed ballots are sorted according to their serial numbers and the parts **A** and **B** (e.g. 100**A** , 100**B**, 101**A**, 101**B**, 102**A**, etc.). In addition, **T** includes information for verifying that the committed values correspond to well-formed ballots. The verification is done by incorporating a novel ZK protocol. Then, EA posts **T** on a *public bulletin board* (BB) and provides a *keyholder* (KH) with the de-commitment information and a *bulletin board authority* (BBA) with the list of pairs of vote-codes andvote-code recording receipts. At the end of the pre-election phase, the working tape of EA is destroyed, for privacy preserving reasons. Note that the KH functionality is distributed to a number of parties via standard secret-sharing to ensure better privacy.

B. Vote-Casting

Vote secrecy in Demos is ensured by the random distribution of the ballots, so that the serial numbers are in no way linked with the voters. When each voter receives a double ballot, she chooses a random side for voting. After the election result is announced, the other part of the ballot will be used for auditing. The double ballot idea for ensuring voting integrity was used in a number of previous systems (e.g., in the Scantegrity system [5]). Then, she sends to BBA the vote-code for the candidate of her choice. This can be done by clicking a button in a user-friendly environment, or manually by typing the vote-code in case the voter does not trust her voting client. The BBA reads the vote-code and if it is valid, it produces the vote-code recording receipt that this vote-code is paired with. It provides the voter with the vote-code recording receipt who can check in her ballot that her vote was correctly recorded by the system. In more detail (refer to Fig. 1 for terminology), the voter can compare the vote-code recording receipt provided by the system to the vote-code receipt appearing next to the party and vote-code of his choice on the ballot's used facet and, thus, if both are identical, be certain that his vote was properly cast through the electronic voting system. An important feature of Demos is that choosing (randomly) one of the two ballot parts for voting, the voter generates (ideally) 1 bit of randomness that is posted on the BB.

We note that after the voter submits the vote-code (using the tablet driven front-end), the system will respond with a vote-code recording receipt as feedback. For example, in Fig. 1, in case the voter votes for party "ΕΛΛΑΣ" the vote-code that will be submitted will be "OIJJ-AGFN-4AUY" while the vote-code recording receipt will be "V605E4". This receipt will appear in the voting interface after the vote-code has been remotely recorded by the system. The voter may check that her vote was received properly by visually verifying that the six digit vote-code recording receipt matches the corresponding receipt for the political party of her choice.

C. Election result computation and verification

After the voting phase has ended, the tally is computed as follows:

1. The KH provides BBA with the de-commitment information and ZK proof information.
2. BBA marks all commitments to the corresponding encoded options (see also Fig. 2 for screenshot of this view).
3. BBA adds (homomorphically) all the marked commitments and opens their sum, which is the election result in encoded form. Finally, it publishes the encoded election result. We note that the result can be efficiently decoded by any party, without the possession of a secret key.
4. Additionally, BBA opens all information for the ballot parts that were used for auditing (Fig. 2), thus revealing the correspondence between vote-codes and parties.

E2E verifiability in Demos is achieved (with high probability)[1] :

1. Because any party can compute the election result and verify the ZK proofs.

[1] We note that the complete security analysis of the system is not the objective of the present paper. However we do present some elements from the analysis in order to give an overview of the system operation. For more information of the demos system please see the web-site http://www.demos-voting.org

2. By the auditing of the ballots: the voter can verify that her ballot was not altered by a malicious party by checking that the perfectly bound opening of the ballot part used for auditing matches the part that the voter obtains. Observe that the malicious EA cannot know in advance which part of the ballot the voter is going to use to vote. Therefore, the EA can guess only with 1/2 probability, which is going to be the part that the voter will choose for auditing. This implies that the probability of altering *t* votes without being detected decreases exponentially in *t*.

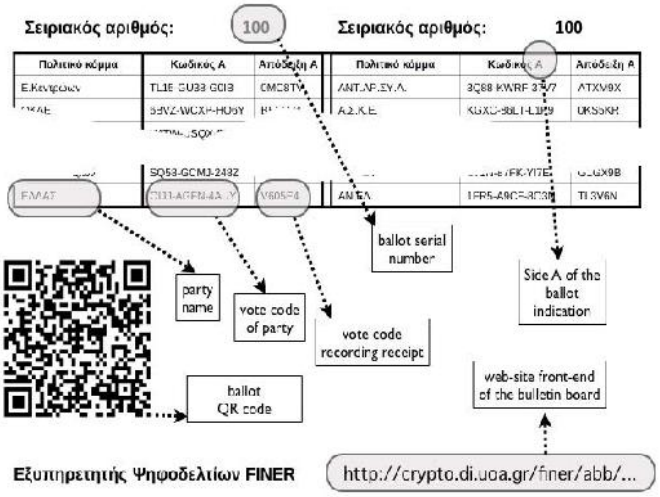


Figure 1. Facet (A) of paper ballot

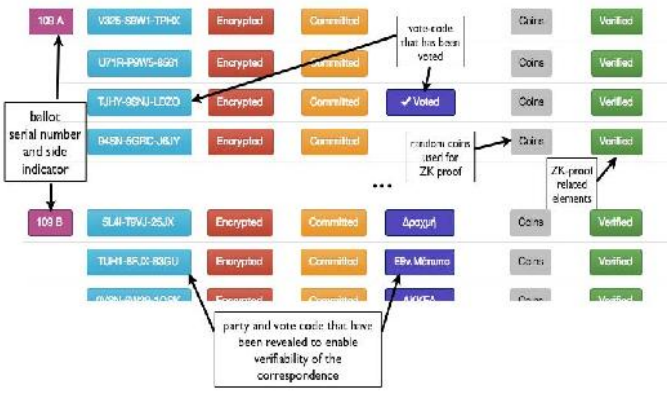


Figure 2. The Bulletin Board at the verification phase

IV. The Pilot Implementation of Demos

In the pilot implementation of Demos, each participant received a paper ballot where in each facet, besides the lists of candidates, vote-codes and vote-code recording receipts, there was a *QR code* (Fig. 1), which, if scanned, lead to a web rendering of the ballot, with an easy to use interface, where candidate parties appeared in buttons the user can click on. In the trial of the system presented below, voters used tablets with cameras to scan paper ballots and voted electronically through the interface described above. The privacy concerns that have been raised when sensitive ballot information is encoded in non-plaintext form, as QR codes, (see [6] for this topic) do not affect our implementation. This is because Demos supports voting by directly typing the vote-codes so that the voter is able to sidestep QR scanning when she does not trust her client. This alternative that our system provides was explained in the participants both on site and via handouts. Furthermore, since all voters voted on site, issues of vote-selling or coercion that are typically linked with remote voting were not raised or examined[2].

As mentioned above, by using their ballot's unique serial number, voters could trace their ballot and check (a) that their vote was properly marked as "voted" and (b) that in the unused version of the ballot all selection codes correspond to the proper candidate parties that were shown in the paper version of the ballot. This covers one of the two parts of the E2E verifiability check of Demos. Note that the complete check requires also the verification of zero-knowledge proofs that may be done by any external observer (including any voter if they wish to do so). This aspect was not tested in our trial (i.e., no third party zero-knowledge verifiers were commissioned), as involving the participants in the technical details of Demos was out of the scope of our experiment.

THE PILOT EXPERIMENT

The trial was conducted on two different polling stations for the 2014 European Elections in the premises of two public schools in highly populated municipalities in the greater Athens metropolitan area. While the actual election procedure was being held inside the school buildings, a set of desks was placed right outside within the guarded courtyard and next to them there were banners that informed the public regarding the trial that was taking place. In each site, two tablets were placed on the desks supported by an elevated Plexiglas stand that allowed for the insertion of the A4 paper ballot underneath (containing the serial number of the "electronic envelope", the codified candidate parties, the *vote-codes* corresponding to them, their *vote-code recording receipts* and the QR code).

[2] Still voters were informed about the functions of the pilot system and its potential application for remote i-voting and, as presented further in the analysis of the distributed questionnaire findings, they were asked whether they would use it to vote from home for national elections. Our system accepts further enhancements to (partially) deal with the issue of coercion that are out of scope for the present exposition.

Four assistants in each site conducted the trial. Assistant A was responsible for calling one out of every four voters that had already participated in the conventional elections, to participate in the e-voting procedure. In case of refusal, Assistant A called the next one and took note of the refusal. Assistant B accompanied the participants to the desks with the tablets, where the other two Assistants were handing them the ballot and explaining them how they could vote via our setting. Only when asked, (in cases where the participants where unfamiliar with scanning a paper) the Assistants would help the participant to scan the ballot under the tablet. Then, keeping a distance to ensure privacy, Assistants C and D, would, if asked to by the participant, offer clarifications or guidance on the use of the e-voting system. Upon submitting their vote, the participants were prompted to a website where they could (optionally) complete the questionnaire online using the same device. The completion of the questionnaire included questions on respondents' socio-demographic backgrounds as well as a number of attitudinal items, measured in five-point Likert scales regarding electronic voting.

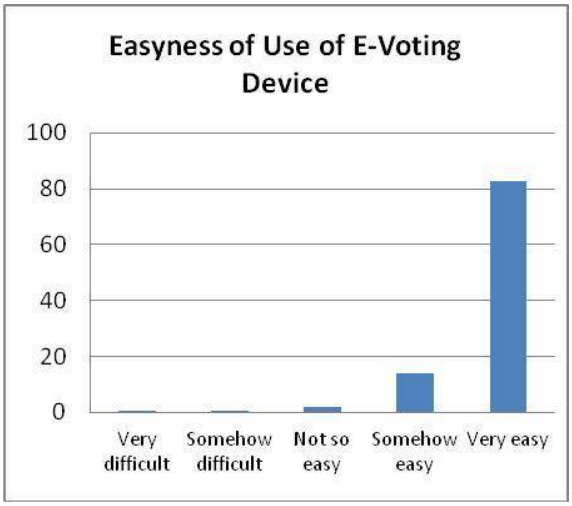
Before leaving, participants were given two leaflets, one containing information about the e-voting system function and features, with emphasis on its procedural safeguards for transparency, verifiability, reliability and security, and another containing a set of simple directions for the successful completion of the verification procedure. A total of 747 people participated in the e-voting trial, while 648 of them filled in the online questionnaire that followed the actual e-voting procedure. Table 1 reports the demographic details of the sample. The sample is skewed in terms of age but mainly in terms of levels of education. Even though this is a typical characteristic of any public opinion survey (e.g. Pew 2012), this means that the aggregate level distribution of attitudes toward e-voting may be higher than what they would appear in the broader Greek population and should be interpreted with caution. The average participation rate was 61.5% in both sites, i.e., about 6 out of 10 voters of the actual voting procedure agreed to participate in the e-voting pilot. The website of the project, (whose address was only publicized in the paper ballots), received 231 unique visits (i.e., a rate of about 30% of the total people that participated) during the next two days. In addition, 21 participants (about 2.8%) chose to make use of the verifiability process and actually locate their ballot assigned to them. It is worth noting that while the verifiability turnout may seem small we consider it satisfactory for our experiment as the verifiability aspect was very briefly explained to each voter (none of which showed any familiarity with this level of secure e-voting design) and the voters were aware of the fact that the pilot election was not binding in any way (and hence one would expect a lower interest in verification than it would have been in case the election was binding). Furthermore, the actual election results were available through other means to all voters (e.g. via regularly conducted exit polls with results broadcasted in the national TV). It is also worth noting that even with as little as 21 verification checks (if done properly) our system would have been capable of providing a reasonable level of election integrity.

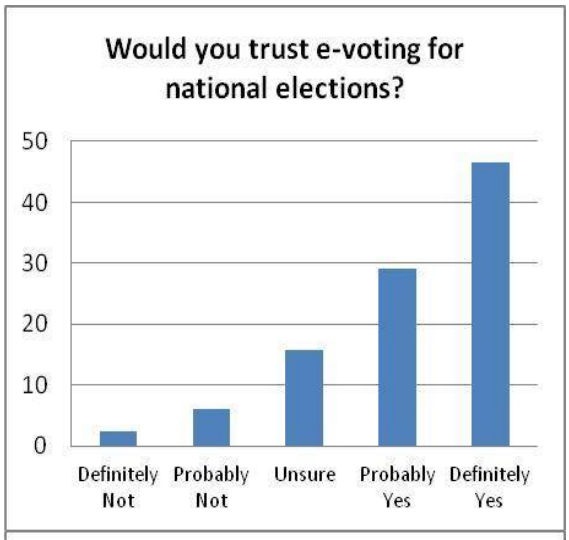
Gender	Percent
Male	50.9
Female	49.1
Age	
15-24	12.8
25-34	16
45-54	24.5
55-64	22.8
65+	7.8
Level of Education	
Up to six years	2
Six to Nine years	3.3
High school graduate	19.3
Some college	13.3
Higher education graduate	41.5
Postgraduate	20.7

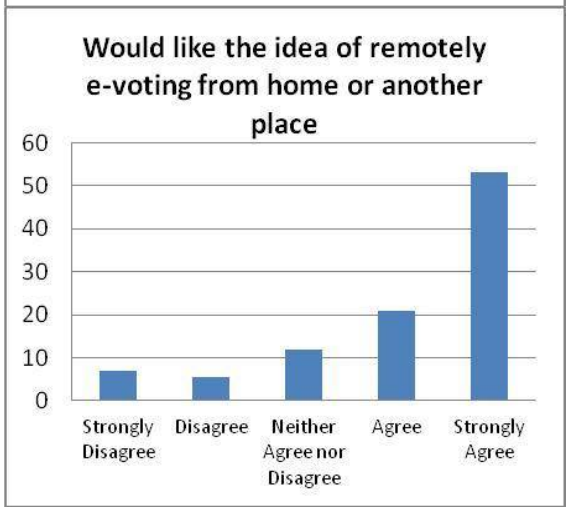
TABLE 1: Demographic Composition of Sample

A. RESULTS

We measured respondents' attitudes toward e-voting through a number of items. Attitudes toward the device were highly positive (Graphs 3-6). Starting with overall satisfaction, nearly 90 percent of respondents answered that they were "somewhat" and "very" satisfied with the electronic voting experience. Moving on to the perceived difficulty of using the e-voting device, 82.7 percent of respondents found its use "very easy", while only 1.2 percent answered that they faced problems using the device. Apart from easiness of use and satisfaction, we measured trust and attitudes toward the adoption of remote electronic voting for national elections. Respondents' attitudes were again very positive: 47 percent of the sample said they would trust an e-voting device such as the one they used for the conduction of European elections, while less than one in ten (8.6 percent) appeared negative toward such an implementation. As for attitudes toward remote electronic voting, roughly three out of four respondents were somehow or very positive toward the prospect of being able to vote in national elections from home with a use of a similar device, while only 12.4 percent appeared dismissive toward this prospect.







Figures 3-6: Distribution of Post-test Respondent Attitudes toward E-Voting

Even though the acceptance of e-voting was quite high in the sample we have reasons to expect that the aggregate distribution masks significant individual-level variation. A number of scholars have argued that the use of electronic voting could possibly create a turnout gap between technologically adept and novices [7-9]. Hence, the argument goes, as the old and less educated are least adept in using technology these population segments will be less likely to vote using an electronic voting device and consequently they may be more skeptical toward the introduction of e-voting devices, and especially remote e-voting devices. Drawing on an e-voting pilot study conducted in the UK in 2003, Norris [7] illustrated that while the option to cast a vote electronically could moderately boost turnout among young voters, it eventually may lead to the suppression of participation among older generations of voters. What is more, since the elder participate in higher rates compared to younger voters, Norris [8] argued that the introduction of electronic voting could lead to an overall decline in electoral turnout.

In order to investigate whether these trends are evident *after* respondents have used electronic voting devices we construct three linear regression models[3], measuring the impact of socio-demographic characteristics (age cohort, gender, level of education) and Internet use (through a dummy variable separating non-Internet users from the rest of the sample) on (a) difficulty using the e-voting device (Model A) (b) trust in e-voting for national elections (Model B) and (c) attitudes toward the prospect of voting from home or another place using a remote electronic voting device (Model C).

[3] In order to ensure that the statistical analysis was not hampered by the discrete nature, nor the non-parametric distribution of the dependent variables all models were re-estimated using complementary log-log regression, an appropriate statistical technique for dealing with highly skewed discrete variables [10]. Results were identical to those reported in the paper in terms of levels of significance and coefficient signs. Same is the case when education is entered as a dummy variable separating those who have attended university from the rest of the sample, with the exception of "easiness of use" where while the education coefficient although positive, falls short of achieving statistical significance.

	Model A		Model B		Model C	
	Easiness of use		Trust		Attitude toward Remote Electronic Voting	
	b	S.E.	b	S.E.	b	S.E.
Male	0,00	0,04	0.01	0.08	-0.07	0.09
Age cohort						
15-24						
25-34	-0,05	0,08	0,50***	0,14	0,53**	0,17
35-44	0,05	0,07	0,73***	0,13	0,60***	0,16
45-54	-0,09	0,07	0,79***	0,13	0,66***	0,16
55-64	-0,08	0,08	1,02***	0,14	0,67***	0,18
65 plus	-0,30**	0,11	1,17***	0,20	0,83**	0,24
Education	0,03**	0,02	-0,01	0,03	-0,01	0,04
No internet access	-0,42***	0,10	-0,07	0,18	-0,09	0,22
Easiness of Use			0,59***	0,07	0,69***	0,09
Adj. R_2	0.12		0.16		0.11	
N	624		620		618	

TableABLE 2: OLS Regression of Easiness of Use, Trust toward E-Voting and Attitudes toward remote e-voting. *(Entries are unstandardized OLS coefficients. Standard errors are reported in the second column.* **: $p < 0.05$; ***: $p < 0.01$)

Beginning with variation in individual-level variation in the difficulty of using the e-voting device, results suggest that educated respondents found it easier to use the device. On the other hand, perceived difficulty was significantly increased for participant categories that are less likely to be familiar with technology, namely respondents aged over 65 years and those who do not use the Internet. Model B reports the respective OLS regression results on trust of e-voting for national elections, using the same independent variables as Model A plus the item measuring perceived difficulty. Results suggest that, all else equal, facility with the e-voting device is associated with general trust toward e-voting, as those who found the use of the electronic voting device easy were more likely to trust the implementation of an electronic voting for general elections. What is striking however is that, all else equal, older aged cohorts appear significantly more trustful toward electronic voting compared to younger age cohorts. This finding that seems paradoxical at first has also appeared in other countries [2] and can be attributed to the fact that younger respondents who are more knowledgeable on issues of technology are more likely to be aware of possible security threats than older and less technologically familiar respondents [2]. Surprisingly, level of education[4] on the other hand is not associated with trust toward electronic voting. The lack of impact of the level of education is against previous findings [2] and needs to be further investigated. Moving on to Model C, which measures variation in attitudes toward remote electronic voting, results suggest that the extent to which one finds remote electronic voting a good idea mainly depends on age and perceived difficulty of using the electronic voting device. Again, as was the case with trust toward e-voting, older respondents appear more positive toward remote electronic voting. What is more, participants who found the use of the e-voting machine easy were significantly more likely to respond that they would like to be able to vote remotely with an e-voting device. Yet it should be noted that the explanatory power of all three models, as indicated by the adjusted R^2 is rather low, meaning that there exist additional latent factors that account for variation in attitudes toward electronic voting in Greece.

CONCLUSION

Electronic voting systems are deemed as a cost-effective alternative for conducting elections, having a promising potential for the quality of democratic representation especially among distinct social groups that may face difficulties accessing polling stations. Yet studies investigating the acceptance of e-voting by the general public remain scarce. This paper advanced the literature on electronic voting by presenting evidence on attitudes toward electronic voting from Greece. Three main conclusions can be drawn from the analysis. First, our results point to the conclusion that acceptance of electronic voting could be fairly high in the general population, bringing additional evidence to confirm previous research by [2] and [3]. This finding however should be interpreted with caution as the sample was skewed in regard with age and level of education, compared to the general Greek population. An additional parameter that may have boosted positive responses is that respondents took part in the trial after having tried the e-voting device. Second, the aggregate distribution of preferences toward e-voting masks significant individual-level variation: Citizens who are already familiar with technology, those who found e-voting easy and older age cohorts were significantly more likely to be supportive of its implementation in national elections. These results appear to substantiate the worry that the advent of electronic voting could possibly create a gap between segments of the population who are familiar with technology and those who are not. On the other hand gender and education were unrelated to e-voting preferences. Third, sociodemographic characteristics and familiarity with technology account only for a small portion of the total variation in acceptance of electronic voting. Future research

[4] It should be noted that the insignificance of education persists with alternative codings as well as when perception of e-voting difficulty and internet use are removed from the model.

could shed more light to the pattern of attitudes toward e-voting from a comparative perspective and further investigate latent parameters that may have an impact on attitudes toward e-voting.

Acknowledgements. The authors gratefully acknowledge the support of the Greek Secretariat of Research & Technology through project FINER, Excellence Programme/ARISTEIA1.

V. REFERENCES

[1] Baldersheim, H., Saglie, J., and Segaard, S. B.. Internet Voting in Norway 2011: Democratic and Organisational Experiences. communication présentée au Congrès mondial de l'Association internationale de science politique, Madrid, 2012.

[2] Alvarez, R. M., Katz, G., Llamosa, R., and Martinez, H. E.. Assessing voters' attitudes towards electronic voting in Latin America: Evidence from Colombia's 2007 e-voting pilot. In E-Voting and Identity Springer Berlin Heidelberg. 2009, p. 75-91.

[3] Sherman, A. T., Carback, R., Chaum, D., Clark, J., Essex, A., Herrnson, P. S. and Vora, P. L. "Scantegrity Mock Election at Takoma Park". In Electronic Voting, 2010, July, p. 45-61.

[4] Chaum, D."Surevote: Technical overview". In Proceedings of the Workshop on Trustworthy Elections, *WOTE*, 2001.

[5] Chaum, D. A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. T. Sherman, and P. Vora. "Scantegrity: End-to-end voter verifiable optical-scan voting". In *IEEE Security and Privacy*, volume May/June, 2008.

[6] Budurushi, J. Stockhardt, S. Woide, M. and Volkamer, M. " Paper Audit Trails and Voters' Privacy Concerns". In Tryfonas, T. and Askoxylakis, I.: LNCS, Human Aspects of Information Security, Privacy and Trust, vol. 8533, p. 400-409, Springer International Publishing Switzerland, June 2014.

[7] Norris, P. "Will new technology boost turnout? Experiments in e-voting and all-postal voting in British local elections". In: Kersting, N., Baldersheim, H., (eds.) *Electronic Voting and Democracy*, New York, 2003, pp. 193–225.

[8] Norris, P. "E-voting as the magic ballot for European Parliamentary elections? Evaluating e-voting in the light of experiments in UK local elections". In Trechsel, A.H. and F. Mendez (eds.) *The European Union and E-voting.* London: Routledge, 2005, pp. 60-90.

[9] Gibson, R. "Internet voting and the European Parliament elections: Problems and prospects". In Trechsel, A.H. and F. Mendez (eds.) *The European Union and E-voting.* London: Routledge, 2005, p. 29-59.

[10] Powers, D. A., Xie, Y. "Statistical methods for categorical data analysis*"*. San Diego, CA: Academic Press, 2000.

Mobile Voting

Electronic Voting with Fully Distributed Trust and Maximized Flexibility Regarding Ballot Design

Oksana Kulyk, Stephan Neumann, Melanie Volkamer, Christian Feier, Thorben Köster
Technische Universität Darmstadt / CASED, Germany
Email: firstname.lastname@cased.de

***Abstract*—One common way to ensure the security in voting schemes is to distribute critical tasks between different entities — so called trustees. While in most election settings election authorities perform the task of trustees, elections in small groups such as board elections can be implemented in a way that all voters are also trustees. This is actually the ideal case for an election as trust is maximally distributed. A number of voting schemes have been proposed for facilitating such elections. Our focus is on a mix net based approach to maximize flexibility regarding ballot design. We proposed and implemented a corresponding voting scheme as an Android smartphone application. We believe smartphones are most likely to be used in the election settings that we consider in the paper. Our implementation also enables voters to remotely participate in the voting process. The implementation enables us to measure timings for the tallying phase for different settings in order to analyze whether the chosen mix net based scheme is suitable for the considered election settings.**

I. Introduction

Recently there has been an increased interest in remote electronic voting, with a focus on large scale elections. However, there are also many smaller scale elections, such as polls in private associations, university environments, committees, and boards with 20 to 30 voters. These boards used to conduct their elections during meetings on paper. Some are planned in advance and others are spontaneous, some use simple yes / no ballots, others more complex options including write in ballots. Elections and polls during meetings are challenging because they happen frequently and people people's mobility has increased. This means that voters are sometimes not present to vote on paper in person. So far technology enables them to participate in public discussions (e.g., over video conference), but they are then either excluded from the voting process or they have to sacrifice the secrecy of their vote in order to participate.

Remote electronic voting would enable them to participate in secret elections, even when they are not physically present. However, well known remote electronic voting schemes such as Civitas/JCJ [1] and Helios [2], [3] are not appropriate as these schemes distribute the duties of registration, voting and tabulation among a number of entities, in advance, requiring a long and time-consuming preparation phase. All this imposes a financial and administrative burden on the election authorities which seems not to be adequate for small scale board elections, in particular spontaneous board elections.

Thus, what is required is a distributed voting scheme, without central servers utilising only the voter's own devices, be it their laptops or smartphones. Note, besides not relying on central servers and not requiring lengthy preparation processes, distributed voting schemes have a further advantage: trust is distributed amongst all voters as all act as trustees.

Correspondingly, our contribution is the proposal of a voting scheme that meets all the above-mentioned requirements of secret elections and polls. The proposed voting scheme is based on existing cryptographic components used in centralized voting schemes such as verifiable mix nets, verifiable secret sharing and threshold decryption.

Furthermore, we implemented the corresponding scheme as an Android smartphone application, allowing voters to participate remotely. Note that we selected smartphone applications as smartphones are most likely to be used in the contemplated election setting and are, as such, the worst-case scenario regarding limitations with respect to computation and network capacity. The implementation enables us to measure timings for the tallying phase for different settings in order to analyze whether the chosen mix net based scheme is acceptable for the considered election settings.

The remainder of this paper is structured as follows: Section II outlines the requirements that were determined to be of relevance for the present election setting. In Section III, we present the design decisions and components selected throughout the voting scheme development process. In Section IV, we describe the composition of these components in terms of a scheme description and evaluate the scheme's security in Section V. In Section VI, we report on the implementation process. Section VII analyzes the scheme's efficiency. Section VIII reviews the related work and Section IX concludes.

II. Requirements

Based on discussions with potential boards (i.e. customers), we identified the following general and security requirements for a suitable voting scheme. Note, these requirements should be considered from a practical perspective since different (often unclear) legal requirements hold in such election settings than for national elections.

A. General requirements

The following general requirements were identified:

Ballot flexibility: It should be possible to conduct elections with ballots of any complexity due to the high spontaneity of corresponding polls:

- Yes/No election
- Multiple candidate selection ("k out of L" election)
- Priority voting (ranking of the candidates)

- Write-in ballots.

Voter flexibility: It should be possible to change the list of eligible voters for each new vote.

Spontaneity: Conducting the election should require as little preparation as possible.

Mobility: The application should run on everyday mobile devices.

Remote participation: It should be possible to cast a vote without being physically co-present with the other voters.

Usability: The system should be usable by non-experts.

Efficiency: The tallying phase should not take more than 15 minutes for 25 participating voters.

Furthermore, it cannot be assumed that it is possible to use PKI.

B. Security requirements

The following security requirements have been identified:

Eligibility: The system should only accept votes from eligible voters.

Uniqueness: Only one vote should be accepted from each voter.

Fairness: The voter should be unable to see the election results, complete or partial, before she casts her own vote.

Vote secrecy: It should be impossible link a voter to his or her individual vote.

Integrity: It should be impossible to replace a cast vote with a vote for another option.

Verifiability: The voter should be able to verify, that the vote she intended to cast is included in the final tally (*individual verifiability*). Furthermore, any third party should be able to verify, that all the cast votes have been tallied correctly (*universal verifiability*).

Robustness: After the votes have been cast, the system should be able to fulfil its functions and tally the votes despite minor errors.

These security requirements should be ensured in the following security model. It is assumed that:

1) More than the half of all the voters are honest and available during the whole voting process i.e. vote casting and tallying. This assumption is justified due to the fact that it would be unreasonable to conduct an election where the majority is corrupt.
2) The devices belonging to honest voters are also reliable and trustworthy, and are not affected maliciously by faults in hardware or software (operating system and voting application). This assumption is justified for the same reason as the previous one. Honest voters without honest devices cannot feasibly run the protocol in an honest way. Note, that in certain settings this assumption might be difficult to ensure. Namely, the smartphones are obviously used privately for other purposes, and might be at risk of infection with malware, especially when the owner is not an expert in mobile security and does not take security precautions. For example, if the OS version on the smartphone is not up-to-date, and the owner often installs apps from untrusted sources, the risks of running the election on such smartphones might be too high, and the application should not be used.
3) Honest users' devices are able to communicate with each other. Similar to the previous assumption this assumption enables honest voters to run the election.
4) No coercion takes place.

To facilitate the second assumption, it is important to embrace diversity in software and hardware. There are several manufacturers of the Android smartphones, thus, there is at least some degree of diversity. The diversity in software can be ensured, if there are different sources and a number of software developers, where the voters can download the voting application from.

Note that we can only guarantee the security requirements for honest voters. However, this holds true for traditional elections as well. For instance, a malicious voter cannot be prevented from forwarding her mail voting material to another person, thus breaking the uniqueness property.

III. Design Decisions

In this section we discuss the cryptographic primitives we used in the proposed voting system.

A. Public Key Infrastructure

As we cannot assume that PKI is in place, part of the voting application is to establish one. We do this by first exchanging the voters' RSA public keys for message authentication, and then exchanging the voters' AES keys for message encryption. One must provide protection against the man-in-the-middle attacks while exchanging the RSA public keys. One way to do this, without relying on certificate authorities and other rather complex preparations, is to use the key exchange based on short authentication strings, as described in [4]. The scheme relies on the existence of an out-of-band channel — namely, the voters should be able to communicate with each other either via physical proximity, or via video or telephone call. This channel is then used to perform manual verification of short strings over such a channel in order to frustrate man-in-the-middle attacks. In order to improve the **usability** of this verification, according to the proposition in [5], the strings have 24-bit length, and are represented as passphrases of three words from the from the PGP Word List [6]. Note, that the communication channels between eligible voters have to be established beforehand in order to execute this scheme; other preparations are not needed, thus increasing **spontaneity**.

After we use the scheme for exchanging the RSA public keys between the voters, thus providing means for message authentication, these keys are then being used to securing communications while establishing symmetric AES keys between each pair of voters via Diffie-Hellman key exchange. For generating the secret parameters in the Diffie-Hellman exchange, the SHA-256 is used as the key derivation function. Thus, means for securing end-to-end encryption are provided.

B. Verifiable secret sharing and threshold decryption

Almost all proposed electronic voting schemes rely on a distributed verifiable secret sharing scheme to generate the election key in a distributed manner and a verifiable threshold

decryption scheme to decrypt individual votes or the sum of all votes in a distributed manner.

A number of secret sharing schemes have been proposed in the literature ([7], [8], [9], [10]), while some of them do not have the means to verify the correctness of the secret sharing, or require the existence of a single trusted instance for key distribution. The scheme that does not have these disadvantages is the one described by Pedersen in [11], [12] and is proven to be IND-CPA secure if used in conjunction with the ElGamal cryptosystem, as shown in [13]. Thus, we decided to use this approach in our application. The corresponding verifiable threshold decryption scheme, which relies on the keys being generated as in [11] is described in [14].

C. Homomorphic tallying versus mix net approach

The approaches most commonly used in electronic voting schemes for preserving the vote secrecy are the homomorphic tallying (e.g. in [15], [14]) and mix net schemes (e.g. in [16], [17]). The first approach relies on homomorphic properties of a crypto system used to encrypt the votes, most commonly, the exponential ElGamal. The homomorphic property is used to multiply the encrypted votes, and then to decrypt the resulting sum. This approach is inefficient for complex kinds of ballots such as priority ranking, and is unsuitable for write-in ballots. Therefore, for ensuring **ballot flexibility** in our application we chose to use the mix net approach.

Two types of mix nets have been proposed: decryption mixnets (e.g. in [18], [16]) and re-encryption mix nets (e.g. in [17], [19]). In order to ensure **robustness** of the scheme, we decided to implement one of the re-encryption mix net schemes. Note, in case of a decryption mix net, one dishonest note can violate robustness.

These schemes also rely on the homomorphic property of an underlying crypto system. A number of entities called the *mix nodes*, the role of which is taken by the voters in our setting, participate in the scheme, whereby each mix node in turn shuffles the list of encrypted ciphertexts $C = (c_1 = Enc_h(v_1, s_1), ..., c_N = Enc_h(v_1, s_1))$ using a secret permutation π and secret randomness values $r = (r_1, ..., r_N)$, outputting the shuffled list $C' = (c'_1, ..., c'_N)$ so that holds:

$$c'_i = Enc_{pk}(1, r_i) \cdot c_{\pi(i)}$$

D. Verifiable mix net schemes

In order to ensure **integrity** and to provide **verifiability**, however, each note has to prove that the input and output set contain the same votes (without revealing π and r). A number of schemes for providing a so called non-interactive zero-knowledge proof of shuffle have been developed ([20], [21], [22], [23], [24]) which mainly differ in their efficiency, degree of vote secrecy, integrity/verifiability as well as robustness. In order to decide which of the proposed proofs is the most appropriate one for our setting, we compare them wrt. efficiency, vote secrecy and integrity/verifiability. For the comparison we apply the following considerations:

- For the efficiency considerations, we consider the number of modular exponentiations E needed for computing the proof of shuffle and for verifying it.
- In order to measure the degree of secrecy of the proposed mix net schemes, we consider the size of *anonymity group* $|A|$. Let $C = \{c_1, ..., c_N\}$ be the list of ciphertexts that results from the final shuffle. Let $A \subseteq C$ be a group of ciphertexts, whereby it is known that the vote of some given voter is in A. Ideally, this group would be the group of all votes cast within the election ($|A| = N$), in which case it is said that a mix net provides *complete* secrecy. Otherwise, if $|A| < N$, the mix net's secrecy is *incomplete*.
- In order to measure the degree of integrity/verifiability of a mix net scheme, we consider the probability p, that the attacker can successfully prove the correctness of an incorrect shuffle. Note, in case p is negligible, the mix net scheme provides *overwhelming* integrity.
- In order to measure the degree of robustness, we consider
  the minimal number of voters t, that should participate and behave correctly during the mixing, in order for it to provide a valid result.

The result of the evaluation according to these considerations is proposed in Table I. As one can see, the schemes that provide the best efficiency, such as the schemes in [20], [21], are seriously lacking in either secrecy or integrity, in particular, for small values of N. As such, the proof of shuffle with the best trade-off between security (secrecy, integrity/verifiability, robustness) and efficiency is the one proposed in [23]; however, since it is covered by patent - to the best of our knowledge, we chose to use the method proposed by Wikström in [24], [25] in our implementation.

TABLE I: Comparison of mix net schemes

PoS	$\|A\|$	E	p	t
[20]	$N/2$	$2N$	50%	$(N/2+1)$
[21]	$complete$	$6\sqrt{N}$	$(\sqrt{N}-1)/N$	1
[22]	$complete$	$12N$	$overwhelming$	1
[23]	$complete$	$2N \log k + 4N$	$overwhelming$	1
[24], [25]	$complete$	$20N + 19$	$overwhelming$	1

k is a divisor of N

E. Proof of Correctness

As shown in [26], ensuring vote secrecy also depends on whether ballot independence is assured: namely, a malicious voter should be unable to cast a vote which is both valid and meaningfully related to a cast vote of another voter. In particular, a group of malicious voters of size f can attempt to break vote secrecy by taking a vote cast by another voter, and casting it as their own vote. Then, after looking at a final result, they could see which vote has been cast at least $f + 1$ times, thus figuring out how the attacked voter has voted. A simple way to prevent this attack is to make the voters prove that they know a corresponding plaintext for a ciphertext message they cast as their vote. For the ElGamal encryption, this can be done by using the non-interactive proof of knowledge of discrete logarithm (described in [27]). Thus, for $c = (a, b) = (g^r, v \cdot h^r)$

with g, h being the ElGamal public keys, the voter has to prove the knowledge of r given a.

IV. Voting Scheme Description

The voting scheme consists of following basic components: verifiable secret sharing, re-encryption mix net, and verifiable distributed decryption. As a crypto system used in encrypting the votes, we chose ElGamal due to its homomorphic properties and its wide use in the selected schemes. Let p, q, g be the corresponding ElGamal parameters, that are publicly available.

1) Ballot initialization: The initiator of the voting composes a ballot that, according to the election type, may consist of the voting question, possible answers, voting rules etc. The empty ballot is then broadcast to all the voters chosen by the initiator, whereby each voter has an option either to agree to participate in the voting, or decline. As a result, the group of voters that is about to participate in this election is formed. In case a set of keys for the election (see Section III-B) has already been generated for this group, the voting proceeds with the *vote casting* stage; otherwise, it proceeds with the *key exchange* stage.

2) Key exchange: This phase consists of generating keys for the election via a verifiable decentralized threshold secret sharing scheme described in [11] with threshold value of $\lfloor N/2 \rfloor + 1$: x_i, the shares of private key that each voter holds, and the jointly computed public key h. The participants also exchange commitments h_i to x_i, which are calculated as $h_i = g^{x_i}$, that are later used for verifiable decryption. The key exchange phase only needs to be performed once for each group of voters; in any further elections conducted by the same group, the previously generated keys can be securely reused.

3) Vote casting: The voters are given a certain time limit, during which they are supposed to cast their vote. The vote v_i is encoded so that it could be used as a plaintext in ElGamal encryption, and e_i is calculated as $Enc_h(v_i, r_i)$ for a random $r_i \in_R \mathbb{Z}_q$. Furthermore, the proof of correctness is used to demonstrate the knowledge of v_i to prevent ballot-copying attacks, as shown in III-E. After (c_i, p_i) have been broadcast by all voters, each voter possesses the initial list of all votes $C_0 = (c_1, ..., c_N)$.

4) Tallying: At the beginning of the tallying phase, the votes are anonymized (Figure 1): this process is divided into N rounds, with fixed execution times. In each round, the voter i applies a mix net scheme to the list C_{i-1} using a random vector $r = (r_1, ..., r_N)$ and a permutation π in order to get a shuffled list $C_i = Enc_h(1, r) \cdot (C_{i-1})_\pi$. She also computes a non-interactive proof of shuffle P_i as described in Section III-D, in order to demonstrate that the shuffle has been executed correctly. After that she communicates the values (C_i, p'_i) to other voters. Then, each one of the remaining voters verifies p'_i, and if it is verified, accepts C_i; if p'_i is not verified, or if the voter i does not send any shuffle result within a round time, sets $C_i := C_{i-1}$. At the end, after all the voters have performed the shuffling, the list C_N is accepted as the final list of anonymized votes. The verifiable decryption scheme is then being executed as described in [14] (Figure 2): for each encrypted vote $c_i \in C_N, c_i = (a_i, b_i)$ each voter j computes the partial decryption share $d_{i,j} = a_i^{x_j}$ using her private key share x_j. (S)he then also computes the non-interactive zero-knowledge proof $p''_{i,j}$ to prove that the secret value x_i used for partial decryption is the same value, that was committed to during key exchange phase. The voters then broadcast their computed values (d_j, p''_j) with $d_j = (d_{1,j}, ..., d_{N,j})$, $p''_j = (p_{1,j}, ..., p_{N,j})$. As soon as any voter gets a threshold amount of partial decryptions and proofs of its correctness $(d_{i,j}, p''_{i,j})$, whereby $p''_{i,j}$ is verified successfully, she can reconstruct the decryption of c_i from the collected values of partial decryption shares. In this way, all the votes in C_N are being decrypted, resulting in values of $V = (v_1, ..., v_N)$. The final result is then tallied according to election rules: as such, for example, if each vote represents a candidate from the given list $v_i \in \{C_1, ..., C_L\}$, the result is the sum of the votes cast for each candidate, $S = (s_1, ..., s_L),\ s_i = |v_j : j = 1, ..., N, v_j = C_i|$.

V. Security Analysis

This section is dedicated to an informal security argument on the presented scheme. To evaluate its security, we identify threats against the security requirements (see Section II-B) and show that the scheme defends against these threats under given assumptions. Note, that the scheme can only provide defence against these threats for the voters with uncorrupted devices, as otherwise the application would just behave according to the attacker's commands, instead of following the scheme.

Eligibility A non-eligible voter can cast the vote in the system, in case there is no authentication in place, or the voter can fake her identity and impersonate an eligible voter. This is not the case if the list of all voters is known in advance, which is ensured in the ballot initiation stage, and if reliable PKI exists, providing means for message authentication and thus preventing identity impersonation. Therefore, it should be impossible for the attacker to impersonate an eligible voter and cast a vote instead of her.

Uniqueness In case no votes from non-eligible voters are accepted, which is ensured via eligibility, a voter can break uniqueness and cast more than one vote, if she can fake her identity and pretend to be another eligible voter. This is impossible due to existing PKI. Thus, it can be ensured that during the vote casting stage, only the voter's first vote (alternatively, only the last one) is accepted.

Fairness In the scheme the fairness property can be broken if a voter is able to reveal others' votes during vote casting. To do this, s/he must be able to decrypt the votes that are broadcast. This is only possible, if at least $\lfloor N/2 \rfloor + 1$ voters collaborate and use their secret keys for decryption. This is impossible according to the assumptions 1-2 in Section II-B; therefore, there is no way for any voter to know the intermediate result at vote casting.

Vote Secrecy The possible ways to break secrecy in the scheme is to either decrypt the cast votes before they are anonymized, or to prevent them from being anonymized. The first way is possible if at least $\lfloor N/2 \rfloor + 1$ voters cooperate maliciously and use their secret key shares for

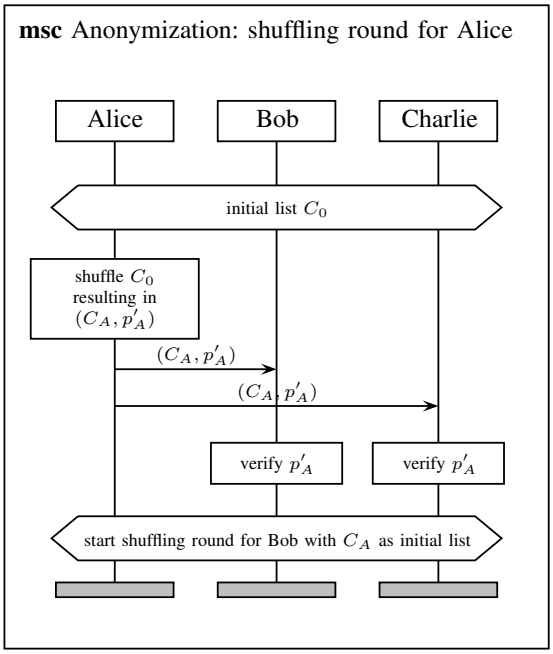


Fig. 1: Anonymization round for $N = 3$

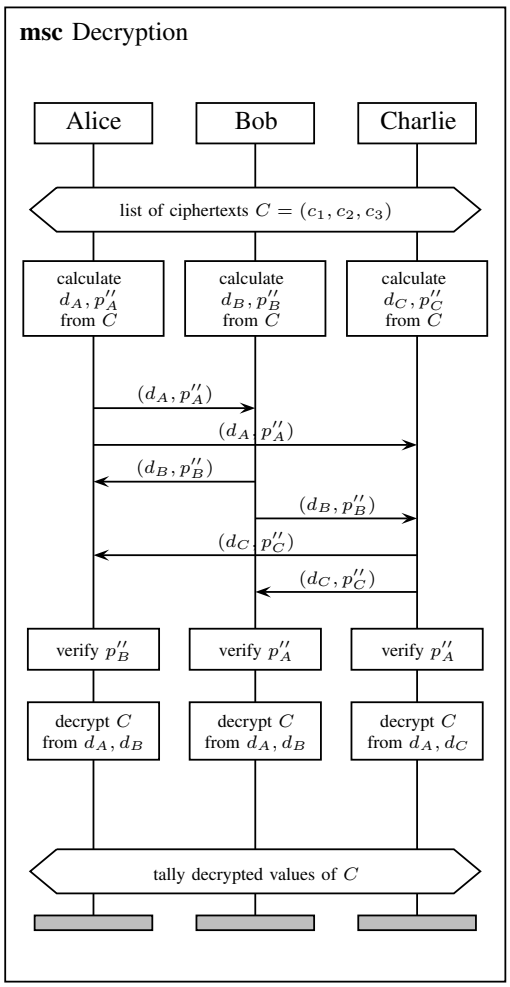


Fig. 2: Decryption for $N = 3$

decryption. The second way is possible if all but one[1] voter decline to perform the anonymization or to keep the correspondences between input and shuffled ciphertexts a secret. Thus, according to assumptions 1-2 in Section II-B, vote secrecy is ensured.

Integrity A way to break integrity and replace some cast vote with another vote, would be either to replace the ciphertext during anonymization stage, or to provide a manipulated partial decryption during tallying stage. This attempts will be detected, however, due to the employment of zero-knowledge proofs during decryption and anonymization, which each voter has to verify before accepting. Therefore, everyone should have the possibility to verify the correctness of the tallying. Thus, any manipulation with the election result will be noticed.

Verifiability Similarly to ensuring integrity, universal verifiability of the correctness of election result is ensured due to non-interactive zero-knowledge proofs that could be verified by anyone using publicly available information. Given universal verifiability, the only way to break individual verifiability would be for the application to cast a vote that is different from the voter's intention. However, due to the assumption 2 in Section II-B, individual verifiability is ensured.

Robustness The result of the voting cannot be decrypted and thus tallied, if only less then $\lfloor N/2 \rfloor + 1$ voters are available and can communicate with each other during decryption. Additionally, the result cannot be tallied without necessarily breaking vote secrecy, if the anonymization of the votes has not been performed correctly, which is possible, as described above, if all but one voter are unable to shuffle the ciphertexts and keep the correspondences between the input list and the shuffled list secret. Therefore, according to assumptions 1-3 in Section II-B, robustness of the system is ensured.

[1] If only one voter is honest, then the public will not know the correspondences between the voter's identity and the vote; however, if all the other voters are dishonest, and each dishonest voter i reveals the correspondences between the ciphertexts in lists C_{i-1} and C_i to the public, the honest voter will be the one who knows how each one has voted. Thus, vote secrecy during anonymization could be ensured only if at least two voters perform their shuffling correctly and do not reveal the correspondences between the ciphertexts.

VI. Implementation

In this section we describe the implementation details of the voting scheme, as well explain particular design decisions

we made.

A. Design Decisions

1) Android app: We developed an application to implement the described voting scheme for Android smartphones. Android is based on a Linux Kernel and is the most widely used mobile operating system. It runs on many different machines which differ in many respects like, for example, screen resolution, CPU power and available memory. The application is designed to support all machines which run Android 4.0 or higher and have more than 512 RAM available.

2) Communication: To establish the communication channels between the voters' smartphones, we had to choose between several options, such as BlueTooth, WiFi-Direct, SMS or instant messaging protocols such as MSN or ISQ. We chose to use XMPP, which is an open-source instant messaging protocol. In advantage to other options, it allows for communications over the network without being in physical proximity to each other, does not place substantial restrictions on message length, and can be extended thus making it easier to adjust for our implementation. To establish a connection to other participating smartphones the Smack API[2] which builds upon XMPP is used. In order for the voters to communicate with each other, the XMPP server has to be available, either as a public server, or as a private server, established by the company. The voters then use their account data on this server to log in the application. As the XMPP protocol communicates via network, **remote participation** is ensured, by enabling every eligible voter to participate in the voting, as long as she has access to network connection, for example, to the mobile internet on her smartphone.

For establishing the PKI we prepared a central server that is used as a "bulletin board" where the initial list of voters is stored. The bulletin board is needed for establishing the PKI only, and is not required on any other stage of voting. This initial list of voters is required in order to enable the initial communication between voter's devices, as voter could send the messages to others only knowing their XMPP account IDs.

This server is relied on with regards to availability only, and does not hold any sensitive information. We use the scheme described in III-A in order to exchange the RSA keys and the AES keys between the voters.

3) Libraries: For implementing the mix net, we did not use the Verificatum implementation by Wikström[3] due to licence restrictions. Instead, the application uses the open-source `unicrypt`[4] library for the mix net implementation. We used the `guava-library`[5] as a utility library e.g. for Base64 encoding. Android ships with a cut-down bouncycastle implementation for cryptographic primitives which only allows symmetric encryptions up to 128 Bit. To support better encryption schemes like 256 Bit symmetric encryption an external library called `spongycastle`[6] is used. Spongycastle is a derivation of Bouncycastle[7], the most popular and extensive Java library for cryptography, which is optimized for Android and renames the packages to avoid classloader conflicts.

B. Walkthrough

We have attempted to make the user interface as simple as possible, requiring only the minimum amount of interaction from the users. We also iteratively improved them due to feedback from colleagues and friends. Note, we plan as future work to evaluate the usability within a user studies.

When starting the application, the voter arrives at the welcome page and logs herself in using her XMPP account. After logging in, the user is referred to the Main Menu (see Figure 3). There, the PKI establishment process can be launched, which concludes when all the voters comparing and verify the passphrases displayed on their screens (see Figure 4). Note, that the PKI establishment scheme is only performed once for each set of voters. It is only repeated when new persons (i.e. new employers, or new boardroom members) are added to the list of eligible voters.

After the PKI has been established, the elections can be conducted. The person who wants to start the election composes and broadcasts the ballot as seen in Figure 5. As all other participants see the invitation and agree to participate, the election starts: if this group of voters starts an election for the first time, the key exchange is being run first. Otherwise, the voters can start with the vote casting, whereby each voter selects her vote and confirms the vote as seen in Figure 6.

After all votes are received the mix net starts anonymizing the votes. As this is the most computationally intensive part of the process, it may take some time. Afterwards the votes are decrypted and tallied and the result shown as seen in Figure 7.

A flow diagram which explains the PKI establishment process (Figure 8), ballot initiation (Figure 9), and voting process (Figure 10) are given, while the captions in bold on the diagrams refer to the steps where the interaction of the voter with the user interface is needed.

C. Fault Handling

We have identified the steps of the voting process, whereby some faults might be present. Most commonly some voters not being present or being unable to communicate with the others might occur. We have already shown, in Section IV, how some of these faults are handled. Furthermore, as shown in Section V, some of these faults, such as the voters failing to produce valid partial decryptions of a vote, could be ignored under the assumptions that we make.

Other faults are the ones that occur during voting phases, that preclude the tallying stage: namely, faults could occur during PKI establishment (i.e. the adversary trying to execute a man-in-the-middle attack), ballot initialization stage (such as voters not responding to the invitation to vote), or vote casting. The diagrams in figures 8,9,10 show the way the application is supposed to handle these faults. As such, for example, the voter who wishes to initiate the election has the option to decide, whether she still wants to start the election if not all of the invited voters respond to her invitation, or to wait some more for the missing voters to respond, or to cancel the election.

[2]http://www.igniterealtime.org/projects/smack/
[3]http://www.verificatum.org/
[4]https://github.com/bfh-evg/unicrypt/
[5]https://code.google.com/p/guava-libraries/
[6]http://rtyley.github.io/spongycastle/
[7]https://www.bouncycastle.org/

Fig. 3: Main Menu

Fig. 4: Establishment of the PKI

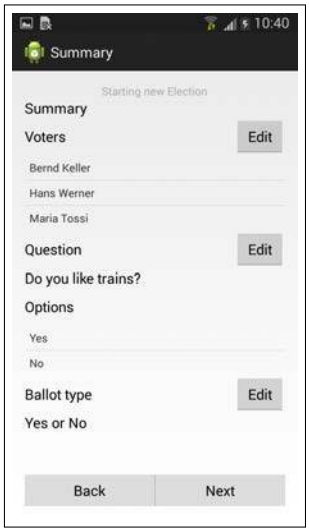


Fig. 5: Summary of the ballot for the new election

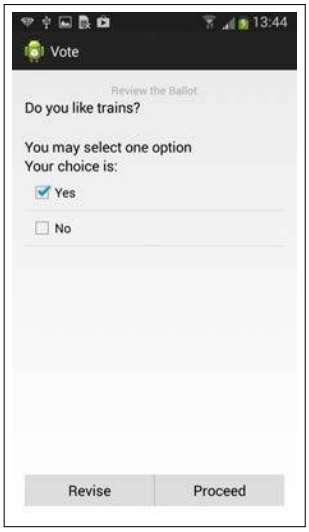


Fig. 6: Overview of a cast vote

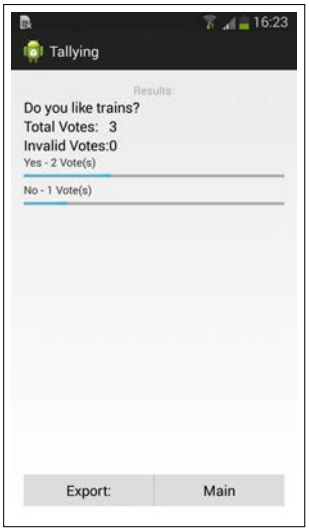


Fig. 7: Election result

Another source of faults during the voting, is the inconsistency of message broadcast. In order to broadcast a message using XMPP, the message has to be sent separately to each receiver. Thus, it makes the system vulnerable to Byzantine faults, whereby a malicious voter can send different messages to different receivers (for example, during broadcasting a cast vote), thus endangering robustness of the voting. One way to solve this problem is to make the voters manually compare the result of each stage (for example, by comparing hash values of a complete list of cast votes at the end of vote casting). Another solution is to implement additional communication schemes that ensure Byzantine Fault Tolerance, such as the schemes described in [28], [29][8].

[8]Note, that some of the methods to implement BFT provide more efficiency at the cost of requiring additional assumptions regarding the amount of faulty nodes f out of total N, most commonly, $f < \lfloor N/3 \rfloor$.

VII. Efficiency evaluation

Without counting the costs of the communication (i.e. signing and verifying the communicated messages, as well as encrypting/decrypting them when needed), the cost of the execution of the scheme in number of required modular exponentiations, with the anonymization stage being the most computationally extensive part, is as follows:

$$26N^2 + 22N + \lfloor N/2 \rfloor + 1 + N(\lfloor N/2 \rfloor + 1) - 1$$

Thus, the efficiency of the voting scheme is $\mathcal{O}(N^2)$. Note that it only depends on the number of the voters, and not on ballot complexity, such as number of candidates or possible options.

As additional computational and communication costs arise in the implementation, which depend on programming tech-

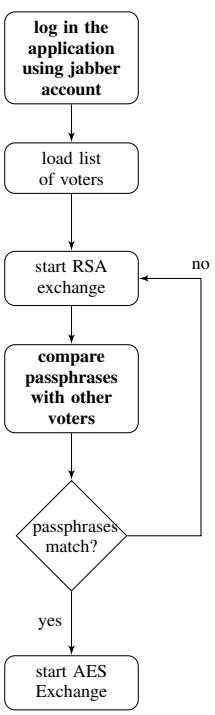


Fig. 8: Establishment of the PKI

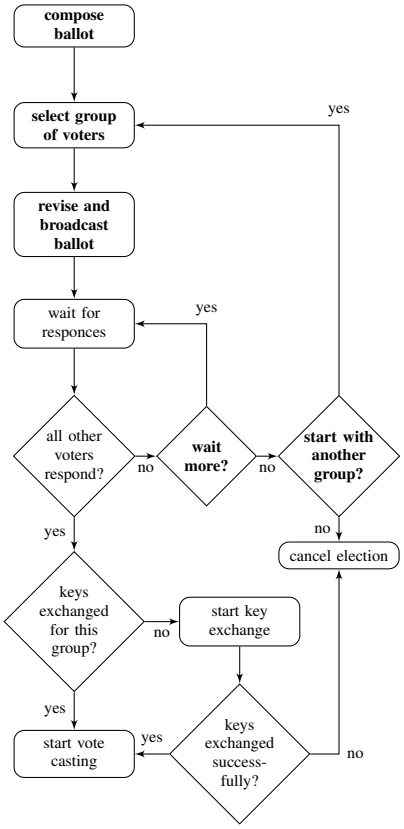


Fig. 9: Ballot Initiation

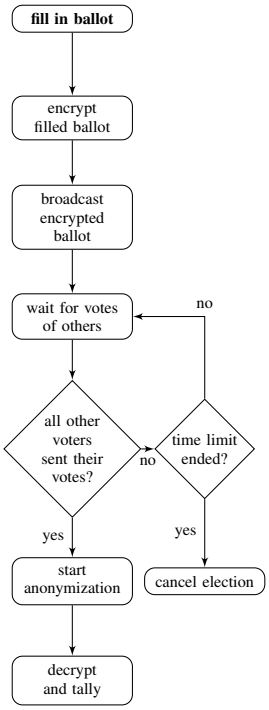


Fig. 10: Vote Casting

niques and network capabilities, we evaluated the performance of the application, by measuring the time it takes to calculate and display the result of voting after the votes have been cast. The application was run on several S3 Samsung smartphones, all in the same room. The "voters" were represented by Gmail accounts with GTalk as the XMPP server for communication, created for test purposes. We did not count the time taken for the PKI establishment stage, since it is only conducted once initially, nor the key exchange stage, since it only has to be executed once for a group of voters. We also did not record the time elapsed during ballot initialization and vote casting, since the time spent on this stage depends mostly on how long the voters take to make their decisions and cast their votes. The key length is as follows: the RSA keys used for message authentication have 2048-bit length, as well as the ElGamal parameters g, p. The ElGamal secret keys, as well as random values used in exponentiations, have 256-bit length.

The resulting times from running the election between $2-5$ voters are given in table II. The times seem linear because of how the cryptographic schemes with several rounds have been implemented in order to achieve synchronization: each round is given a fixed amount of time, during which it is expected for all computations to be complete. Thus, this time is chosen as an upper limit for the computations - namely, for the mix net scheme, the duration of one shuffling round is set such as one should be able to complete the shuffling of 25 ciphertexts, which includes calculating and verifying the corresponding proofs of shuffle. Thus, the time spent on anonymizing the votes is $\mathcal{O}(N)$ for $N \leq 25$. The time for decrypting the votes is $\mathcal{O}(N^2)$, but it is relatively small compared to the anonymizing stage. Thus, extrapolating the times for 25 voters[9], we can assume that the election will last slightly less then 12 minutes on such devices.

TABLE II: Execution times of tallying stage

Number of voters	Average execution time (ms)	Average execution time (min)
2	65764.5	1.10
3	85152.7	1.42
4	109375	1.82
5	129702.6	2.16

VIII. Related Work

A number of schemes for decentralized voting with distributed trust has been proposed in the literature. Among them are the works in [15], [30] and [14], which were implemented in the *MobiVote* application. The security model of these schemes is similar to the one that we describe in this paper, namely, the security of the scheme depends on the majority of the voters and their voter devices being uncorrupted. However, the schemes in question employ homomorphic tallying, thus being less suitable for complex ballots. An Android application for spontaneous decentralized voting in classroom setting has been proposed in [31]; the approach, however, does not ensure verifiability. A scheme for decentralized voting

[9]We used the polynomial trend line function in Excel.

has been described in [16], and then expanded in [32]. The scheme uses mix net scheme for anonymizing the votes; however, it relies on all the voters being uncorrupted during the anonymization stage for ensuring robustness and integrity, which is a disadvantage compared to our approach.

IX. Conclusion and Future Work

We have presented a scheme for decentralized voting with distributed trust, and an application that implements this scheme, thus enabling secure elections in small groups. We have shown that this application fulfills the security requirements of eligibility, uniqueness, fairness, vote secrecy, integrity, verifiability, robustness, as well as the general requirements of ballot flexibility, voter flexibility, spontaneity, mobility, remote participation that we have set as our goal. As a future task, we will work on the usability of the application, conducting user studies and improving the user interfaces. As part of improving usability, we will work on further improving efficiency of the application. This includes (1) using the fact, that the mix net scheme developed in [24] is specifically designed with an "offline" and "online" phase, whereby the offline phase is the computationally extensive one, and can be executed before the election actually starts. Currently, these two phases are executed one directly after another during vote anonymization. The offline phase, however, could be completed in advance, during the idle time of the protocol, when no other extensive computations are being executed, thus making the tallying phase substantially faster. Furthermore, (2) efficiency of the vote anonymization will be further improved by only requiring a subset of all voters to participate as mix nodes. We have shown that at least two honest voters are needed to ensure vote secrecy during vote anonymization. Thus the set of shufflers must contain at least two honest voters. According to our assumptions, at most $\lceil N/2 \rceil - 1$ voters are dishonest. Adding two honest honest voter upon $\lceil N/2 \rceil - 1$ results in the fact that the minimal number of voters that need to act as mix nodes is $\lceil N/2 \rceil + 1$. In order to determine the shufflers for each election, a common reference string to generate randomness can be used. One could instantiate the common reference string by a cryptographic hash value of all the votes cast in the election, then using it as an input in a deterministic function that outputs a sequence of shufflers. Another way would be to sort the list of all voters in the election according to canonical order, and choose the first $\lceil N/2 \rceil + 1$ from the sorted list. Another way to improve efficiency will be to use elliptical curves instead of integer groups, in which case additional considerations on how to encode votes are necessary.

Another direction of future work is to discuss the issue of people using same or similar smartphones as well as people all installing the software from the same vendor or download it from the same platform.

Finally, we will also have a closer look to the robustness of the application. In particular, we will implement the Byzantine Fault Tolerance scheme in order to make communication more reliable. An efficient way to do this, that requires more than two thirds of honest nodes, is described in [28]. Another, way to implement the Byzantine Agreement is described in [29]. Although this way is less efficient, it does not require changes in security model, and can be applied if more than half of all the voters are honest, provided that the means of message authentication are in place.

Acknowledgment

This paper has been developed within the project 'BoRoVo' Board Room Voting - which is funded by the German Federal Ministry of Education and Research (BMBF) under grant no. 01IS12054 and within the project ComVote, which is funded by the Center for Advanced Security Research Darmstadt (CASED), Germany. The authors assume responsibility for the content. We also thank the reviewers for their valuable comments that helped to considerably improve the quality of this work.

References

[1] Clarkson, M.R., Chong, S., Myers, A.C.: Civitas: Toward a secure voting system. In: IEEE Symposium on Security and Privacy, IEEE Computer Society 354–368

[2] Adida, B.: Helios: Web-based open-audit voting. In van Oorschot, P.C., ed.: USENIX Security Symposium, USENIX Association 335–348

[3] Karayumak, F., Olembo, M.M., Kauer, M., Volkamer, M.: Usability analysis of helios-an open source verifiable remote electronic voting system. In: Proceedings of the 2011 USENIX Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. USENIX. (2011)

[4] Nguyen, L.H., Roscoe, A.: Efficient group authentication protocol based on human interaction. In: Proceedings of Workshop on Foundation of Computer Security and Automated Reasoning Protocol Security Analysis. (2006) 9–31

[5] Farb, M., Burman, M., Chandok, G., McCune, J., Perrig, A.: Safeslinger: An easy-to-use and secure approach for human trust establishment. Technical report, Technical Report CMU-CyLab-11-021, Carnegie Mellon University (2011)

[6] Zimmermann, P.R.: Pgpfone: Pretty good privacy phone owner's manual. MIT, http://web. mit. edu/network/pgpfone/manual (1995)

[7] Shamir, A.: How to share a secret. Communications of the ACM **22**(11) (1979) 612–613

[8] Feldman, P.: A practical scheme for non-interactive verifiable secret sharing. In: Foundations of Computer Science, 1987., 28th Annual Symposium on, IEEE (1987) 427–438

[9] Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Foundations of Computer Science, 1985., 26th Annual Symposium on, IEEE (1985) 383–395

[10] Benaloh, J.C.: Secret sharing homomorphisms: Keeping shares of a secret secret. In: Advances in CryptologyCRYPTO86, Springer (1987) 251–260

[11] Pedersen, T.P.: A threshold cryptosystem without a trusted party. In: Advances in CryptologyEUROCRYPT91, Springer (1991) 522–526

[12] Pedersen, T.P.: Distributed provers and verifiable secret sharing based on the discrete logarithm problem. DAIMI Report Series **21**(388) (1992)

[13] Cortier, V., Galindo, D., Glondu, S., Izabachene, M.: A generic construction for voting correctness at minimum cost-application to helios. IACR Cryptology ePrint Archive **2013** (2013) 177

[14] Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. European transactions on Telecommunications **8**(5) (1997) 481–490

[15] Khader, D., Smyth, B., Ryan, P.Y., Hao, F.: A fair and robust voting system by broadcast. In: EVOTE'12: 5th International Conference on Electronic Voting. (2012)

[16] DeMillo, R.A., Lynch, N.A., Merritt, M.J.: Cryptographic protocols. In: Proceedings of the fourteenth annual ACM symposium on Theory of computing, ACM (1982) 383–400

[17] Benaloh, J.: Simple verifiable elections. In: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, USENIX Association (2006) 5–5

[18] Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM **24**(2) (1981) 84–90

[19] Jakobsson, M., Juels, A., Rivest, R.L.: Making mix nets robust for electronic voting by randomized partial checking. In: USENIX security symposium, San Francisco, USA (2002) 339–353

[20] Jakobsson, M., Juels, A., Rivest, R.: Mix nets robust for electronic voting by randomized partial checking. USENIX security symposium (2002)

[21] Demirel, D., Jonker, H., , Volkamer, M.: Random block verification: Improving the norwegian electoral mix-net. In Manuel J. Kripp, M.V., Grimm, R., eds.: 5th International Conference on Electronic Voting 2012 (EVOTE2012). Volume 205 of LNI - Series of the Gesellschaft für Informatik (GI)., Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC, Gesellschaft für Informatik (July 2012) 65–78

[22] Groth, J.: A verifiable secret shuffle of homomorphic encryptions. Journal of Cryptology **23**(4) (May 2010) 546579

[23] Bayer, S., Groth, J.: Efficient zero-knowledge argument for correctness of a shuffle. In: Advances in Cryptology EUROCRYPT. (2012)

[24] Terelius, B., Wikström, D.: Proofs of restricted shuffles. In: Progress in Cryptology–AFRICACRYPT 2010. Springer (2010) 100–113

[25] Wikström, D.: A commitment-consistent proof of a shuffle. In: Information Security and Privacy, Springer (2009) 407–421

[26] Smyth, B., Bernhard, D.: Ballot secrecy and ballot independence coincide. In: Computer Security–ESORICS 2013. Springer (2013) 463–480

[27] Schnorr, C.P.: Efficient signature generation by smart cards. Journal of cryptology **4**(3) (1991) 161–174

[28] Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI. Volume 99. (1999) 173–186

[29] Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) **4**(3) (1982) 382–401

[30] Hao, F., Ryan, P.Y., Zieliński, P.: Anonymous voting by two-round public discussion. IET Information Security **4**(2) (2010) 62–67

[31] Esponda, M.: Electronic voting on-the-fly with mobile devices. ACM SIGCSE Bulletin **40**(3) (2008) 93–97

[32] Alkassar, A., Krimmer, R., Volkamer, M.: Online-wahlen für gremien. DuD Datenschutz und Datensicherheit **8**(29) (2005)

Scroll, Match & Vote: A Coercion-Resistant Mobile Voting Interface

Carlos Ribeiro
Inesc-id and
Instituto Superior Técnico
Universidade de Lisboa
Email: carlos.ribeiro@tecnico.ulisboa.pt

Rui Joaquim
SnT
University of Luxembourg
Email: rui.joaquim@uni.lu

Gonçalo Pereira
Inesc-id and
Instituto Superior Técnico
Universidade de Lisboa
Email: goncalo.pereira@tecnico.ulisboa.pt

***Abstract*—Mobile Internet elections are appealing for several reasons: they promise voter convenience, lower abstention rates, and reduce costs. However, there are a number of trust issues that prevent them from becoming ubiquitous, the most relevant of which is the possibility of voter coercion at the time of the vote. Other issues, such as the trustworthiness of both the services running the election and the mobile voting platform (usually the voter's computer or smartphone), are also major barriers to mobile Internet elections adoption.**

The proposed "Scroll, Match & Vote" (SM&V) interface aims to overcome these trust issues, while attempting to ensure the usability required for wide adoption. The SM&V interface may be coupled with previous e-voting solutions to ensure end-to-end verifiability and collusion resistance [1], while adding coercion resistance to a degree similar to that of several coercion-resistant e-voting systems. The SM&V interface requires the use of a device with Internet connection and multitouch screen.

Prior to voting, the voter is required to register in a controlled precinct sometime between several months before the voting phase to immediately preceding the vote. In the voting phase, the voter is shown two lists side by side on the device. One list contains all the candidates' names and the other list shows voting codes. One of the voting codes is correct; the others are false. The voter casts her vote by scrolling one or both lists and matching her chosen candidate with the correct code. The voting phase may take place anywhere with an Internet connection, even in the presence of coercers.

I. Introduction

Internet elections have been a research subject for many years with a number of interesting results, several of which are being piloted worldwide [2], including on actual binding elections [3], [4]. The arguments in favor of Internet elections are obvious: i) increased voter convenience and participation, ii) greater tally accuracy and speed, and iii) reduced costs, among others. However, the arguments against Internet elections are also pertinent: i) the insecure voting-platform problem, which results from the use of multipurpose devices owned and managed by the voter [5]; ii) the lack of transparency resulting from the nonexistence of physical votes and the possibility of collusion between the digital devices participating in the election; and iii) the nonexistence of private voting precincts paving the way for several coercion scenarios.

Carlos Ribeiro was supported by Suspect, PTDC/EIA-CCO/122542/2010
Rui Joaquim was supported by the Fonds National de la Recherche, Luxembourg (grant INTER/SNF/11/11).

The widespread use of smartphones with ubiquitous Internet access has emphasised some of these advantages and disadvantages. While it is even more convenient for the voter to vote on her own smartphone, it is also easier for the coercer to influence her vote, given that the voter may vote anywhere. In spite of this, one of the most common reasons for the failure of voting experiments is the lack of usability; voting systems that are too complex are doomed to fail, even if they are able to overcome all the security problems noted above [6].

Scroll, Match & Vote (SM&V) is a coercion-resistant interface that may be coupled with an end-to-end verifiable and collusion-resistant voting protocol, like MarkPledge3 (MP3) [7], to build an Internet voting system that compares advantageously with other Internet voting systems [1], [8].

Elections are usually constrained in time and space, i.e. they must be conducted on the specified election day and in controlled precincts. This double constraint is one of the sources of abstention, given that not everyone is available to be at a specific place on a set date during certain hours. Removing either of these constraints is highly problematic. If the election takes too long (i.e. several months), the democracy suffers because some voters vote with much less information than others. Early voting and postal voting are seen as exceptions rather than as the rule. Removing the space constraint is also difficult because it usually means loosing coercion resistance [8]. The current proposal follows the path of JCJ/Civitas [9], [8] and splits the two constraints such that the space constraint and the time constraint do not apply to the same action. The voter must register at a private booth without tight time constraints (within a span of one or two months) and must vote on election day without any space constraints (with the exception of having an Internet connection).

The SM&V interface assumes that the voter owns a mobile Internet device with a multitouch screen (hereafter referred to the voter's smartphone).

The next section describes the complete voting process, while section III states and discusses the security properties of the system and section IV discusses usability properties. We conclude in section V.

II. SM&V Voter Interaction

From a voter's perspective, the voting machine is her smartphone, although, as described below, the actual ballot creation may be performed by an applet running inside a

UICC, a secure SDCard, or any other secure element (SE) in order to ensure confidentiality of the vote (cf. [10]).

The voter process is divided into three phases: the registration phase, the voting phase, and the verification phase.

The **registration** phase is the most complex phase of the voting process. It begins following the election initialization by the electoral commission and ends just before votes are cast, i.e. it can be done even on election day.

When SM&V is coupled with MP3, the voter is required to challenge the voting machine during registration using random values. These can be generated prior to the registration in the form of printed 2D codes by the voter herself, by an online helper organization, or even by a coercer, provided that he is not colluding with the voting machine (i.e. the UICC or the SDCard). Other end-to-end verifiable voting protocols will require slightly different interactions. The following describes the registration process for SM&V coupled with MP3.

To register, the voter should takes her smartphone to a private booth prepared especially for this purpose and presses register on her smartphone voting application (screen I in Figure 1). She will then be asked to: choose the election (screen II); read one of the 2D codes with her smartphone camera (screen III) and, tap her phone against a special device, within the private booth, dubbed "Pledge Display Device" (PDD) (screen V), whose only purpose is to build an untappable channel between the voter and the voting machine, in order to display a short secret voting code to the voter: the "pledge".

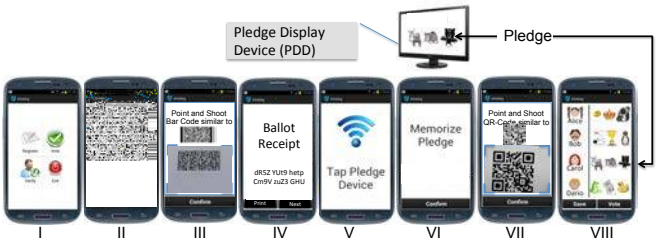


Fig. 1. Registration procedure.

The PDD owes its existence to the untrustworthiness of the voter's smartphone. Being a multipurpose device with many different applications running, it is assumed that anything displayed on its screen may be leaked to a coercer. The PDD's only purpose is to receive, decrypt, and display the "pledge". It does not know anything else about the voter; therefore, it cannot compromise the voter's privacy. Still, to ensure that using false PDDs is impossible, the "pledge" is sent to the PDD encrypted with the PDD's key, which is provided for the voting machine in a certificate signed by the electoral commission.

After tapping the smartphone on the PDD, the voter is asked to memorize the "pledge" showed in the PDD (screen VI), and read the second 2D code (screen VII). For usability purposes, the two 2D codes should be different types (e.g. a PDF417 and a QR code).

In the final step of the registration phase the voter's smartphone displays two scrollable lists side by side (screen VIII). The list on the left displays the names of the candidates, while the list on the right displays an equal number of sequences of symbols, one of which is the "pledge" shown in the PDD. To prevent coercion, the voter should also memorize a few other sequences of symbols to be used as false voting codes in case of coercion. The registration ends either by saving the generated ballot or by engaging immediately in the voting phase.

Voting is accomplished by sliding one or both lists on the screen so that the chosen candidate and the sequence of symbols with the "pledge" become aligned (they can be visible or not, provided that they are aligned), and pressing "VOTE". Without knowing the "pledge", no one next to the voter will able to tell which candidate the voter has chosen. Given that the voter is able to mislead the coercer about the sequence encoding the "pledge", a coercer will not be able to tell which candidate the voter is voting for.

In the **verification** phase, the voter checks to see if her vote was counted as she intended by verifying that her signed vote is in the poll, the 2D codes published match the printed ones, and that the vote is counted for the chosen candidate, which is done by checking a copy of her ballot. The copy of the ballot shown is similar to screen VIII of Figure 1, with the difference that it cannot be changed (the rotation is signed); the voting codes become verification codes for the end-to-end protocol and the voter may verify that the "pledge" is next to the chosen candidate. This verification process can be done using the mobile voting app, but it is recommended that the voter use another Internet device with a simple web browser connected to a Helper Organization (HOs) that she trusts. In addition to showing the vote to the voter, HOs run the necessary cryptographic checks to ensure that the verification code next to each candidate was not tampered with, and that the overall tally is correct [10].

III. Security Properties and Trust Model

The purpose of the proposed interface is to add coercion resistance to an "end-to-end verifiable" protocol, thus building a system that ensures both properties simultaneously. We have chosen the MP3 protocol for its high degree of soundness and performance, although the same exercise may be done with other end-to-end verifiable protocols. The connection between the SM&V interface and the MP3 protocol requires a slight change in the voting process (the voter casts her vote only after the generation of the MP3 receipt, which is different from the standard MarkPledge protocol usage), and MP3 verification codes are also used as voting codes, but it can be demonstrated that the overall system maintains the MP3 security properties [10].

MP3 ensures the integrity of votes cast, even if every entity is compromised, provided that there is at least one honest HO and, that, at the very least, a subset of the trustees are honest. However, it does not ensure confidentiality of the vote unless the voting machine is not compromised. Coercion resistance is not possible without vote confidentiality; therefore, SM&V ensures coercion resistance only if the voting machine is not compromised, which in our case requires that the SDCard or UICC is not compromised.

In addition to the voting machine's integrity requirement, SM&V also requires that PDDs do not disclose the "pledges" to anyone but the voters, and that only legitimate registration precincts own certified PDDs, i.e. PDDs with a certificate

signed by the election committee for that specific election. Finally, the channel between the PDD and the voter cannot be tappable, which is the most difficult requirement to satisfy, given that any one with a camera is able to record and transmit what is being displayed by the PDD within the voting booth. In spite of the difficulty, this is a common assumption of most voting protocols, including the traditional paper-based voting.[1]

With the satisfaction of the above requirements, SM&V is able to ensure simultaneous "end-to-end verifiability" and limited coercion resistance. In particular, an SM&V system is vulnerable to the following coercion attacks:

- **Randomization** - An attacker may force a voter to vote randomly, preventing the voter from voting for her the chosen candidate.
- **Forced-Abstention** - An attacker may obtain a proof of abstention by looking at the tally and verifying whether there is a vote for the coerced voter. Therefore, anyone may force a voter to abstain and then verify wether she has complied.
- **Pre-attack surveillance** - A coercer may learn with some probability the "pledge" of a voter by checking the cast ballot and learning the code next to the voter's likely chosen candidate. After learning the "pledge", the coercer may force the voter to revote for another candidate. The coercer does not know, for sure, however, wether the learned "pledge" is the correct "pledge". This vulnerability is shared with Civitas [8].

The only mitigation mechanism provided by SM&V in response to any of these attacks is to allow the voter to override her e-vote by voting physically at a voting booth.

IV. Usability Discussion

Usability is a major issue in any voting system but assumes a specific relevance in end-to-end voting systems, where the voter distrusts her voting machine and is, therefore, required to handle a more complex voting interface.

SM&V requires the voter to be able to memorize the "pledge" for a long period (sometimes over a month) and to be able to distinguish it from the remaining voting codes. From a usability perspective, a short sequence of symbols simplifies memorization; however, the length of the sequence depends on both the number of different voting codes and the number of different symbols. The number of different voting codes is set accordingly with the level of security required and the size of the ballot; more voting codes imply a lower probability of guessing the "pledge". Therefore, using short and memorable sequences implies the use of large sets of symbols, which complicate distinguishability, unless the chosen set of symbols is carefully designed so that each symbol is clearly distinguishable from the others.

According to Bertin [11] there are eight visual variables that are used by humans to distinguish symbols: shape, size, color, brightness, pattern, orientation and horizontal and vertical positions. Symbols that differ in more variables are easier to distinguish from each other; therefore it is possible to use large sets of symbols provided that they differ in as many of these variables as possible. On the other hand, long-term memory in humans beings works better with semantic information [12] rather than with abstract information, which seems to indicate that symbols representing concrete concepts are preferred over abstract ones.

TABLE I. Distribution of subjects by age and gender

	Gender			
Age	Male		Female	
15-24	5	(11.4%)	8	(18.2%)
25-49	22	(50%)	6	(13.6%)
50-64	2	(4.5%)	1	(2.3%)
> 64	0	(0%)	0	(0%)

TABLE II. Memorization techniques reported by the voters

Memorization technique	Number	
Sequence of symbols of the "pledge"	15	(29.4%)
Non-repeating symbol of the "pledge"	12	(23.5%)
Candidate in front of the "pledge"	8	(15.6%)
"Pledge" position within the ballot	7	(13.7%)
History with the symbols of the "pledge"	3	(5.88%)
Other	6	(11.8%)

We have run tests with a set of 128 different symbols, varying in both color and shape, representing 128 different objects and animals[2]. Both the "pledge" and the voting codes in the ballot are shown as combinations of three of these symbols (with a maximum of 2^{21} combinations), which results in a highly sound election (cf. [1] for soundness proofs).

The quality of the chosen set of symbols was tested by performing an experiment with 45 different subjects, with the distribution of age and gender shown in Table I. Two-thirds of the subjects were university students or had university degrees; one-fifth had only a basic education and the remaining subjects had completed secondary education. Each of the subjects was shown a sequence of three symbols similar to the "pledge" and a list of sequences of three symbols similar to the ballot. Then the subjects were asked to find the "pledge" in the ballot and memorize both the "pledge" and the position where it appears in the ballot. A copy of the ballot was given to the subjects, who were also instructed not to make any mark or written annotation about the "pledge". Finally, a month later, the subjects were asked to point to the "pledge" in the ballot.

The results were promising, although there is still some margin for improvement; only three of the 45 subjects (6.7%) were not able to point to the "pledge" within the ballot, resulting in $93.3\% \pm 6\%$ correctness for a confidence level of 0.9. However, the reasons for these errors were completely unrelated to gender, age or education level. Of the three subjects who forgot the "pledge", two mistakenly identified one symbol for another in their "pledge" (the same pair of symbols which were too much similar) and the third mistakenly identified a voting code similar to the "pledge" of a previous experiment. These two types of mistakes confirmed the relevance of carefully thought-out choice of symbols and

[1] Notice the official warnings against selfies taken inside the booth in the 2014 European elections.

[2] Taken from the popular game *Categories*.

revealed that consecutive elections should not share the same set of symbols. Both problems may be easily solved.

The voters who chose the correct "pledge" reported using several techniques in order to memorize it (Table II). While some reported to have memorized all three symbols in the "pledge" (29.4%), others memorized just one symbol that they found was not repeated in any other position in the ballot (23.5%). Still others memorized the name of the candidate that was in front of the "pledge" when the ballot was saved (15.6%). Finally, some memorized the position of the "pledge" in the ballot (13.7%). Note that a few voters used several memorization techniques.

Another interesting result was the subjects' perceptions of the level of difficulty of the task; the task was perceived to be much more difficult than it actually is. While 28.9% of the subjects stated, at the beginning of the experience, that they were expecting to fail (i.e. forgetting the "pledge"), the reality is that only 6.7% (three subjects) forgot, and the mistake was due more to an error in the experiment than to the inability of the voters. This error in subjects' perceptions of the difficulty of the task may result from modesty, i.e. the voter may not want to boast about her ability to memorize the code without testing how difficult it is. However, it may also result from not correctly perceiving the task they were asked to perform. In fact, several voters showed surprise when they were told that they could keep the "pledge" written in the ballot together with the other codes and would just have to memorize which of them it is the "pledge", and that they could even refresh their memory from time to time, if they want to do so.

Some subjects also reported that they would prefer a different set of symbols, such as numbers or letters. In fact, SM&V may be adapted to use several sets of symbols in the same election, provided that the voter chooses the set of symbols to use prior to seeing the "pledge" (to avoid a covert channel). With such an option, one of the sets of symbols could be specifically designed for color-blind voters. Nevertheless, it is expected that some voters will forget the "pledge" or be uncertain of it, yet they should not be prevented from voting. In SM&V, a voter may register again and receive another "pledge" or may even decide to invalidate her Internet registration and vote using the traditional paper-based ballot or any other voting methods, i.e. SM&V may coexist with other voting methods, leaving to the voter the choice of which method to use.

The experiment also demonstrated that using SM&V for simultaneous election and multiple-choice elections has additional usability challenges. It is clear that asking voters to memorize one "pledge" for each election will result in a major usability problem. On the other hand, using one "pledge" for every simultaneous elections will result in a security problem. One solution is to create a ballot with every possible combination of choices and ask the voter to choose one combination of candidates. Such large ballot would not only require a different interface to be shown and manipulated by the voter but also a huge number of different verification codes. Finding a large-enough distinguishable set of symbols is a challenge by it self. A possible solution is to use a combination of nouns and verbs, creating random sentences like "Tickets Flood Chicken". Such verification codes can easily reach 10^9 combinations ($10^3 nouns \times 10^3 verbs \times 10^3 nouns$), and can be alphabetically ordered, which is enough for most elections ($\mathrm{O}\left(10^6\right)$) but not all (e.g. Chicago voters in 2000 had 78 choices to make).

V. Conclusion

Although secure mobile Internet elections are a difficult goal to achieve, and there is still a long way to go until all relevant properties are attained simultaneously, particularly resistance to *surveillance attacks*, we believe that SM&V is a step in that direction.

SM&V leaves room for further development in terms of both security and usability. From a security point of view, the most important evolution would be the resistance to surveillance attacks within the voting booth. While eliminating these attacks may be difficult, it might be possible to raise the bar for the attacker by incorporating touch sensitive channels (e.g. cold and hot surfaces) between the voter and the Secure Element generating the vote. From a usability point of view, it is also possible to envision several developments. The current interface is not able to manage multiple-choice and simultaneous elections. Both problems may be solved by the same solution, given that multiple-choice elections can mimic multiple simultaneous elections, and several solutions are currently being tested.

References

[1] R. Joaquim, C. Ribeiro, and P. Ferreira, "Eviv: an end-to-end verifiable internet voting system," *Computers & Security*, vol. 32, pp. 170–191, 2012.

[2] R. Krimmer, S. Triessnig, and M. Volkamer, "The development of remote e-voting around the world: A review of roads and directions," in *E-Voting and Identity*, ser. LNCS. Bochum, Germany: Springer Berlin / Heidelberg, October 2007, vol. 4896, pp. 1–15.

[3] G. Schryen and E. Rich, "Security in large-scale internet elections: a retrospective analysis of elections in estonia, the netherlands, and switzerland," *Information Forensics and Security, IEEE Transactions on*, vol. 4, no. 4, pp. 729–744, 2009.

[4] Ministry of Local Government and Regional Development, "e-vote 2011 - project web site," September 2012, http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658.

[5] A. D. Rubin, "Security considerations for remote electronic voting," *Commun. ACM*, vol. 45, no. 12, pp. 39–44, Dec. 2002. [Online]. Available: http://doi.acm.org/10.1145/585597.585599

[6] A.-M. Oostveen and P. Van den Besselaar, "Security as belief: user?s perceptions on the security of electronic voting systems," *Electronic voting in Europe: Technology, law, politics and society*, vol. 47, pp. 73–82, 2004.

[7] R. Joaquim and C. Ribeiro, "An efficient and highly sound voter verification technique and its implementation," in *E-Voting and Identity*. Springer, 2012, pp. 104–121.

[8] M. Clarkson, S. Chong, and A. Myers, "Civitas: Toward a secure voting system," in *IEEE Symposium on Security and Privacy*. Oakland, CA, USA: IEEE Computer Society, May 2008, pp. 354–368.

[9] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Proc. of the 2005 ACM workshop on Privacy in the electronic society*. Alexandria, VA, USA: ACM, November 2005, pp. 61–70.

[10] C. Ribeiro, Joaquim, and G. Pereira, "Scroll, match & vote: An e2e coercion resistant mobile voting system," INESC-ID, https://www.inesc-id.pt/ficheiros/publicacoes/10160.pdf, Tech. Rep. 14, May 2014.

[11] J. Bertin, *Semiology of graphics: diagrams, networks, maps*. Wisconsin: University of Wisconsin press, 1983.

[12] F. I. Craik and R. S. Lockhart, "Levels of processing: A framework for memory research," *Journal of verbal learning and verbal behavior*, vol. 11, no. 6, pp. 671–684, 1972.

Proceedings EVOTE2014
TUT Press

ISBN 978-9949-23-685-5 (PDF)
ISBN 978-9949-23-688-6 (publication)

This conference is one of the leading international events for e-voting experts from all over the world. One of its major objectives is provide a forum for interdisciplinary and open discussion of all issues relating to electronic voting. Cumulatively, over the years 2004, 2006, 2008, 2010, 2012 and 2014 more than 550 experts from over 35 countries have attended this conference to discuss electronic voting and related topics. In so doing, they have established Bregenz as a regular forum and point of reference for the scientific community working with e-voting. This is the proceedings volume of the tenth anniversary of the first conference and contains 17 papers accepted for presentation at the conference.

printed by TUT Press, Tallinn