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

# 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**

205

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?

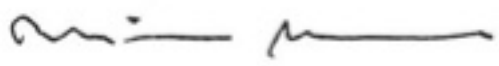
One thing is for certain. New governance models in a plugged-in world will no doubt entail greater demands for transparency and accountability.

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

**Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm**
*Overview* ..... *18*

Session 1: Verifiable Internet Voting in Norway: Lessons Learnt

**Ida Sofie Gebhardt Stenerud, Christian Bull**
*When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting* ..... *22*

**Jordi Barrat, Michel Chevalier, Ben Goldsmith, David Jandura, John Turner, Rakesh Sharma**
*Internet Voting and Individual Verifiability: The Norwegian Return Codes* ..... *36*

Session 2: The Technology behind the Norwegian Internet Voting

**Jordi Puigalli, Sandra Guasch**
*Cast-as-Intended Verification in Norway* ..... *50*

**Denise Demirel, Hugo Jonker, Melanie Volkamer**
*Random Block Verification: Improving the Norwegian Electoral Mix-Net* ..... *66*

Session 3: Verification of E-voting

**Craig Burton, Chris Culane, James Heather, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, Zhe Xia**
*A Supervised Verifiable Voting Protocol for the Victorian Electoral Commission* ..... *82*

**M. Maina Olembo, Anna Kahlert, Stephan Neumann, Melanie Volkamer**
*Partial Verifiability in POLYAS for the GI Elections* ..... *96*

Session 4: Coercion Resistant E-voting Systems

**Oliver Spycher, Reto Koenig, Rolf Haenni**
*Achieving Meaningful Efficiency in Coercion-Resistant, Verifiable Internet Voting*.... *114*

**Jérome Dossogne, Frederic Lafitte, Olivier Markowitch**
*Coercion-Freeness in E-voting via Multi-Party Designated Verifier Schemes*..... *128*

## Session 5: Auditing and Testing of E-voting

**L. Jay Aceto, Michelle M. Shafer, Edwin B. Smith III, Cyrus J. Walker**
*Internet Voting System Security Auditing from System Development through Implementation:Best Practices from Electronic Voting Deployments* ..... *146*

**Mark D. Phillips, Richard W. Soudriette**
*Testing Democracy: How Independent Testing of E-Voting Systems Safeguards Electoral Integrity* ..... *160*

## Session 6: Practical Experience with Internet Voting

**Ardita Driza-Maurer, Oliver Spycher, Geo Taglioni, Anina Weber**
*E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons* ..... *174*

**Tiphaine Pinault, Pascal Courtade**
*E-voting at Expatriates' MPs Elections in France* ..... *190*

## Session 7: Practical Experience with E-voting

**Carlos Vegas**
*The New Belgian E-voting System* ..... *200*

**Guillermo Lopez Mirau, Teresa Ovejero, Julia Pomares**
*The Implementation of E-voting in Latin America: The Experience of Salta, Argentina from a Practitioner´s Perspective* ..... *214*

## Session 8: Analyzing E-voting: Survey and Results

**Nina Boulus-Rødje**
*Mapping the Literature: Socio-cultural, Organizational and Technological Dimensions of E-voting Technologies* ..... *228*

**Jessica Myers, Joshua Franklin**
*Interpreting Babel: Classifying Electronic Voting Systems* ..... *244*

**Jurlind Budurushi, Stephan Neumann, Melanie Volkamer**
*Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-binding Elections and Approaches Proposed in Scientific Papers* ..... *258*

Session 9: New Developments and Improvements to E-voting

**Marc Teixidor Viayana**
*Electronic Voting and Null Votes: An Ongoing Debate* ..... *274*

**Dalia Khader, Ben Smyth, Peter Y. A. Ryan, Feng Hao**
*A Fair and Robust Voting System by Broadcast* ..... *286*

**H. Serkan Akilli**
*Mobile Voting as an Alternative for the Disabled Voters* ..... *302*

**Jonathan Ben-Nun, Niko Fahri, Morgan Llewellyn, Ben Riva, Alon Rosen, Amnon Ta-Shma, Douglas Wikstrom**
*A New Implementation of a Dual (Paper and Cryptographic) Voting System* ..... *316*

# 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:

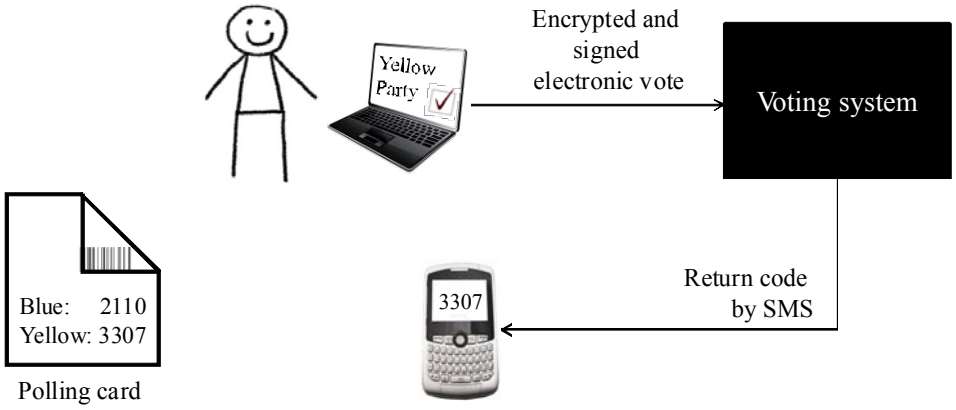



Fig. 1: A functional overview of the voting process

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.

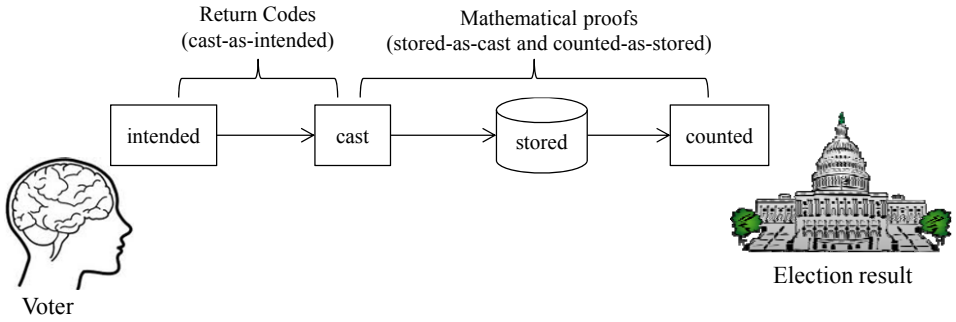



Fig. 2: The vote life cycle and the verification steps

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.

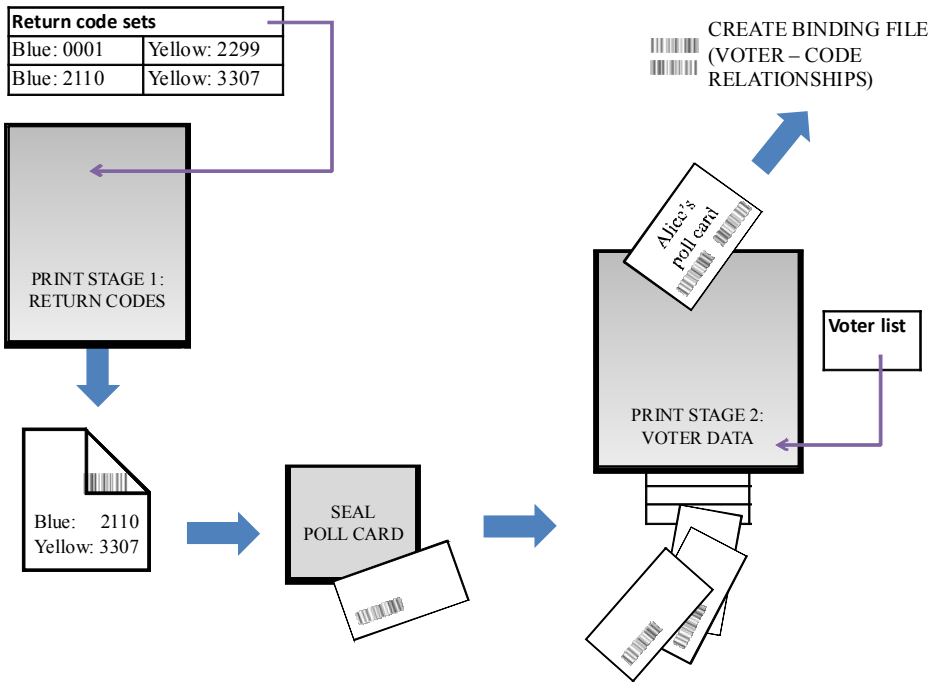



Fig. 3: The poll cards printing process

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.

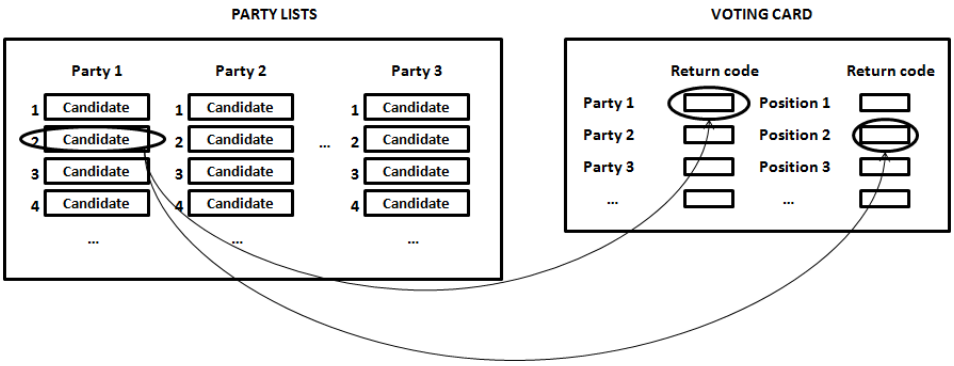



Fig. 1: Cast-as-intended verification with voting cards

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.

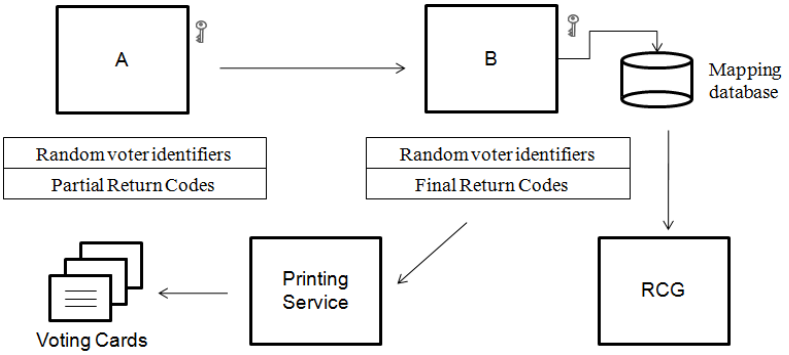



Fig. 2: Return code information generation during the configuration phase

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:

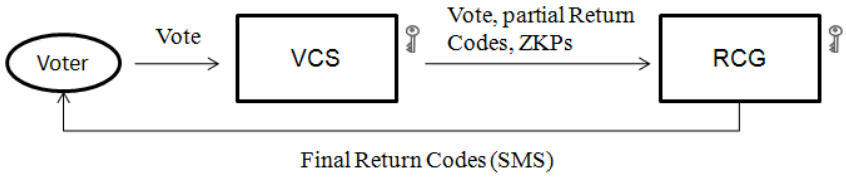



Fig. 3: Return code generation during the voting phase

## 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.

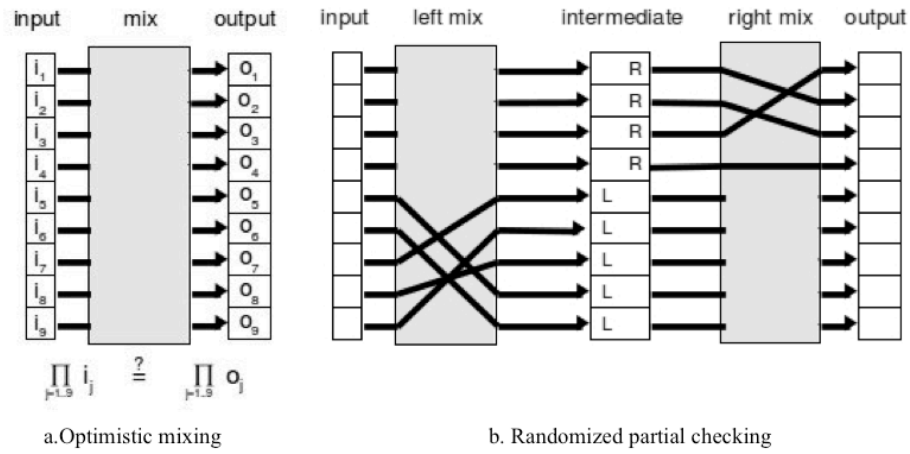



Fig. 1: Two approaches to trading verification for efficiency in mix nets

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 $\pi$, 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.

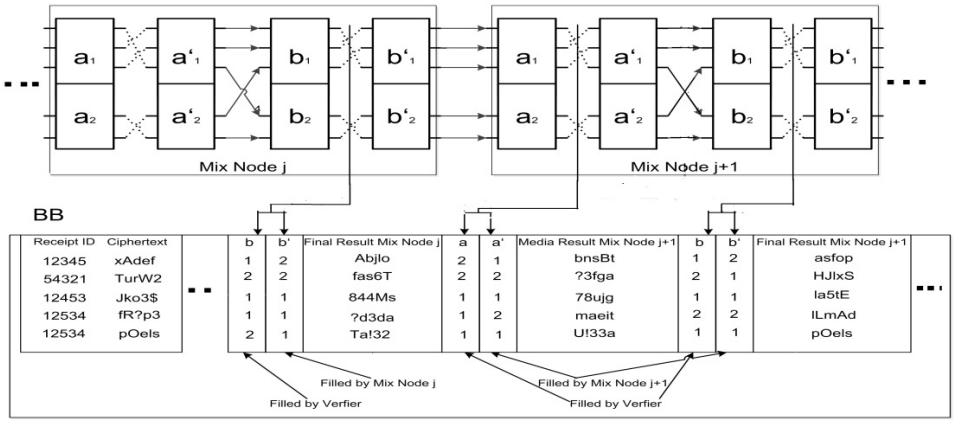



Fig. 2: Verification of one Mixnode for 5 ciphertexts, 2 blocks

*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, $\alpha$ 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 $\alpha$ random blocks (with $\alpha$ 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 $\alpha$ , 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 $\alpha$ -component of the ciphertext and two times $n/2$ for $\beta$ -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 $\alpha$ = 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.

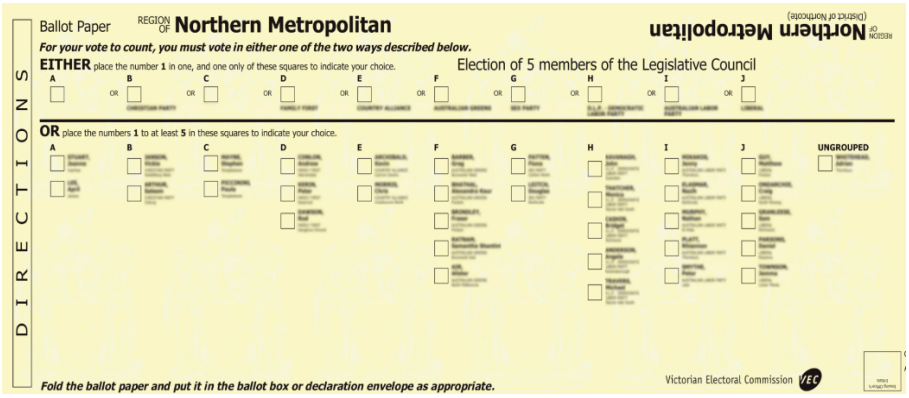



Fig. 1: Ballot paper for the Victorian Legislative Council

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 | $\theta_E$ |
| Bravo | $\theta_B$ |
| Alpha | $\theta_A$ |
| Delta | $\theta_D$ |
| Charlie | $\theta_C$ |
| $\{P\}$ | |

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.

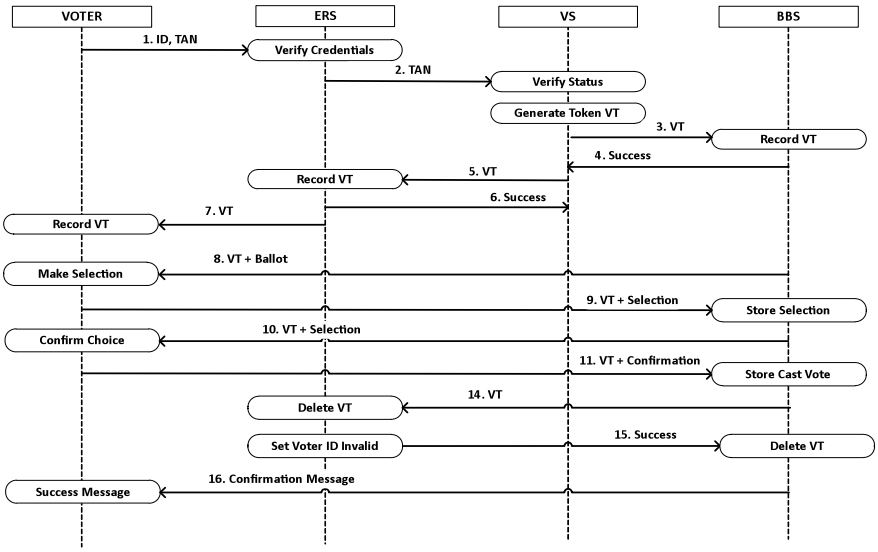



Fig. 1: A simplified view of the voting phase in POLYAS

**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 ($\delta$). 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 $\Gamma$ 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 $\Gamma$.

In [KTV10], Küsters et al. introduce their notion of a measure for quantifying coercion-resistance. They define the degree of coercion-resistance $\delta$ 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 $\Gamma$ 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 $\Gamma$ is to be expected in real life. On the other hand, since voters are also uncertain about $\Gamma$, 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 $\Gamma$ 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 $\delta$.

Given the exclusion of $\Gamma$ from adversarial uncertainty, some parameterizable, JCJ-related protocols can be configured to achieve a degree of coercion-resistance that depends solely on the estimated $\Gamma$. 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 $\Gamma$ hadn't been assumed. Finally, it cannot be estimated whether coercion based on $\Gamma$ 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, $\delta$ 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 $\delta$-coercion resistant system. Obviously, small $\delta$ values are what we are looking for.

The protocol we are about to introduce is $\delta$-coercion resistant in a parameter $\beta$. We will compare its performance with others under parameters $\beta$ that yield equal degrees of coercion-resistance $\delta$, where $\delta$ signifies the reduction of coercion-resistance compared with the JCJ-protocol. Remarkably, unlike $\Gamma$, we are able to quantify $\delta$ 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 $\delta$-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 $\delta$-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 $\varepsilon$ 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 $\beta$ denotes the security parameter underlying the degree of coercion-resistance $\delta$, 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 $(\sigma, i)$, whereas we use the terms $\sigma$-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 $\alpha_\sigma$ and $\alpha_i$, 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 $(\sigma, i)$, 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 $\alpha_\sigma$ and $\alpha_i$. 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 $\sigma$. This is done indirectly by proving knowledge of $\alpha_A$. We thereby exclude the attempt to cast an illegitimate vote by undetectably copying and re-randomizing $\sigma$-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 $\sigma$-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 $\sigma$ 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 $\delta$-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 $(\sigma, i)$ 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 $\sigma$-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 $\mathrm{PET}$ to the first two components. If the algorithm comes back as *true*, $A$ is an encryption of a valid $\sigma$-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 $\sigma$-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 $\Gamma$. 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 $\sigma$-credential), coercion will become even more difficult. However, we adhere to the strict model proposed in the JCJ paper.

[8] The precise value of $\delta$ 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 $\sigma$-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.

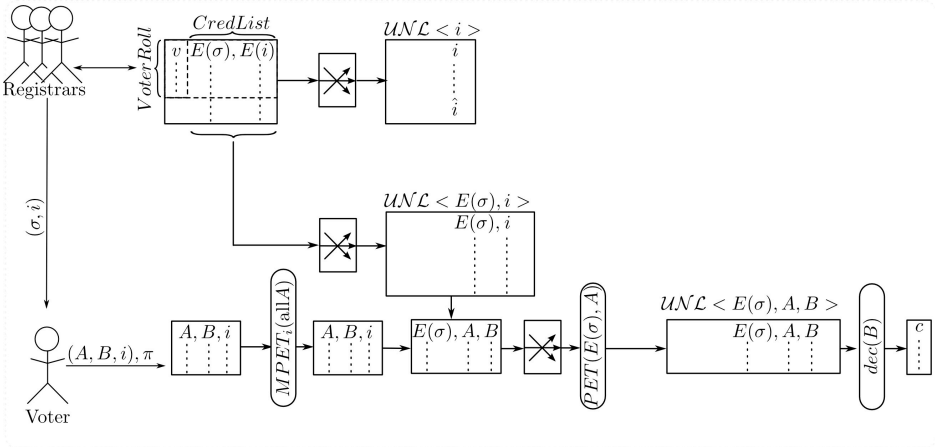



Fig. 1: Basic protocol

**Credential Retention.** As implied above, our scheme allows voters to re-use the same credential $(\sigma, i)$ 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 $\sigma$-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 $\Gamma$, 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 $\Gamma$ 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 $\sigma$-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 $\sigma$-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 $M - PET$.

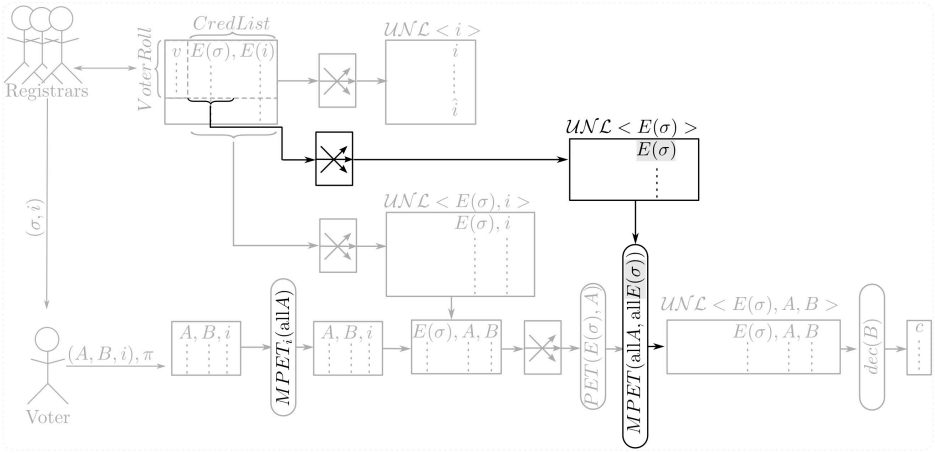



Fig. 2: Enhancement to the basic protocol to achieve full protocol

## 4 Efficiency

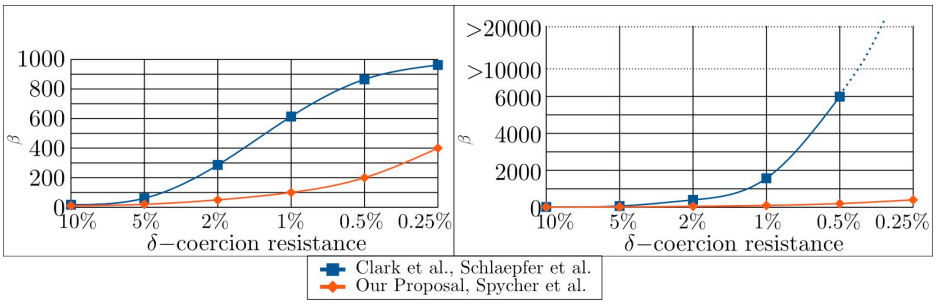



Fig. 3: The two drawings show the parameter $\beta$ dependent on the degree of coercion-resistance $\delta$. The diagram on the left shows the case for 1000 voters and 1000 votes on the voting board, the one on the right 100000 voters and 100000 votes on the voting board.

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 $\beta$.[10] In the case of Clark et al., the *computation time on the voter's platform* scales in the parameter $\beta$. 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 $\beta$, 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 $\beta$ 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 $\beta$ 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 $\beta$, 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 $\delta$, 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 $\sigma$ 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 $U = \{u_1,\ldots,u_w\}$, 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 $x \in \{0,1\}^*$.

$S \subset U$ 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 $\sigma_m$ 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 $\eta$.

### 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:
$\text{Setup}_{KGS}(\eta)$: Inputting security parameter $\eta$ generates a master public key (MPK) and a master secret key (MSK). The MPK is transmitted to each user $u_i \in U$.

$\text{KeyGen}_{KGS}(\text{MPK},\text{MSK})$: 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 $\sigma_m$ 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 $\sigma_m$, 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 $\eta$ 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($\sigma$,$m$,$mpk$) Anybody can use this algorithm to check whether $\sigma$ 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 $\sigma_m$ 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 $\sigma_m$, 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 $\sigma_m$ 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 $\sigma_m$ through $\sigma'_m$: $m^{-k_{S_i}y} = \sigma_m/\sigma'_m = m^d/m^{d+k_{S_i}y} \bmod n$

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 $\sigma_m$ 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.

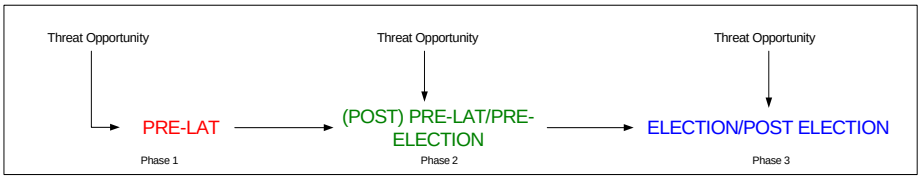


Fig. 3.: Simplistic Election Management Workflow Threat Model

## 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.

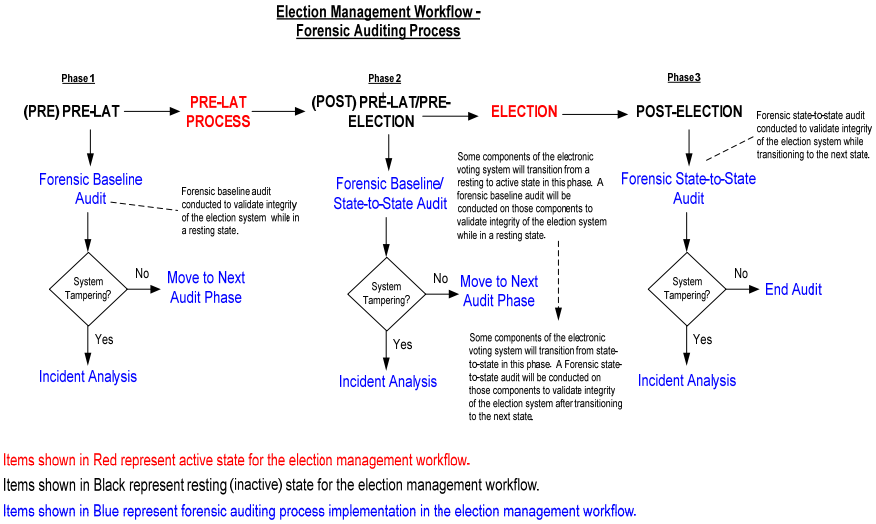



Fig. 4.: Election Management Workflow & Forensic Auditing Process

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.

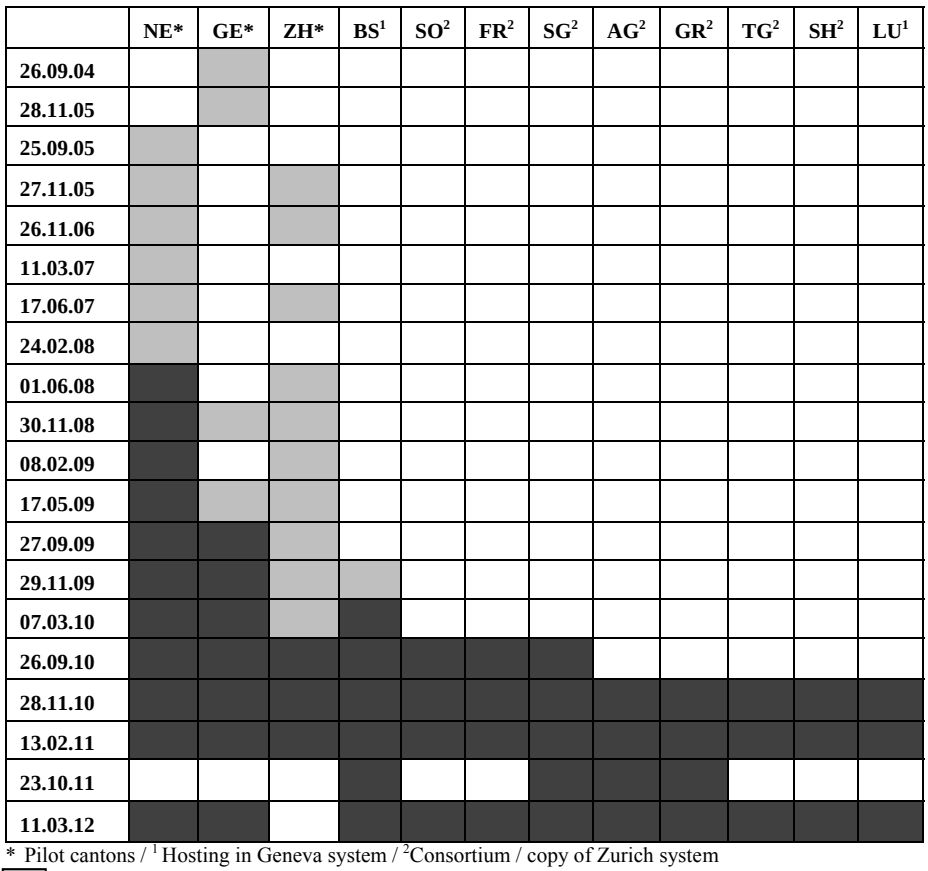
[37] The user group has the competence to decide upon the development/modification requests coming from the partners; deal with the organisation of votes/election, the technical specifications, fix priorities, and handle costs; decide the functional modifications of the system which can impact the hosted 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.

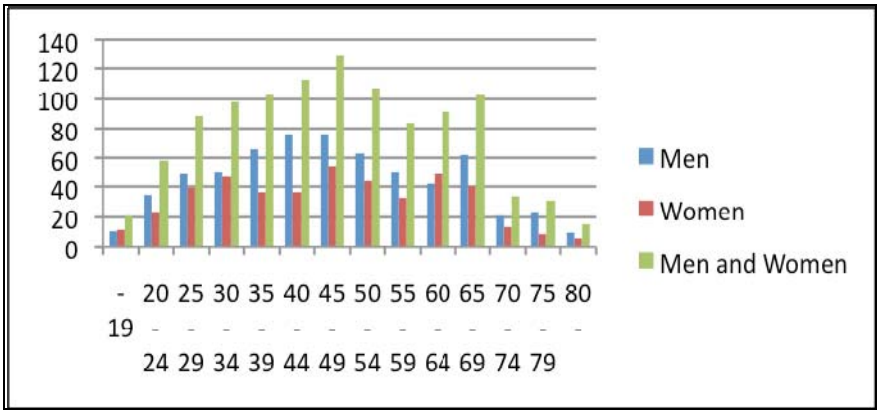



Fig. 2: Voter participation among Swiss abroad registered in canton Grisons using e-voting, by age group (Source: Grisons Cantonal Chancellery)

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

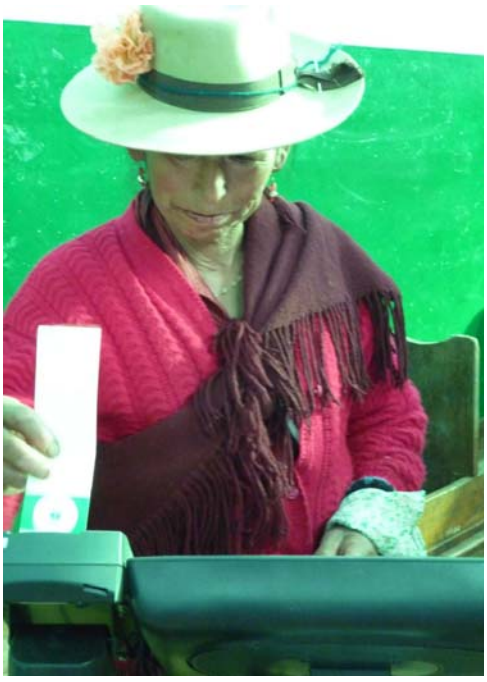
CIPPEC Foundation
Callao 25, 1,
1425 Buenos Aires, Argentina
jpomares@cippec.org

**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).

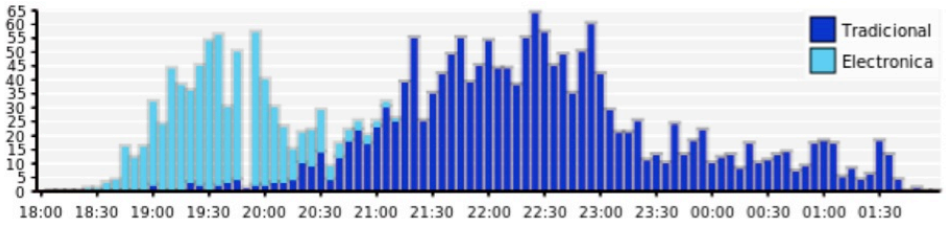



Fig. 1: Histogram of Number of polling tables' tally of votes received by the Electoral Tribunal by type of voting system, source: Electoral Court of the province of Salta

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.

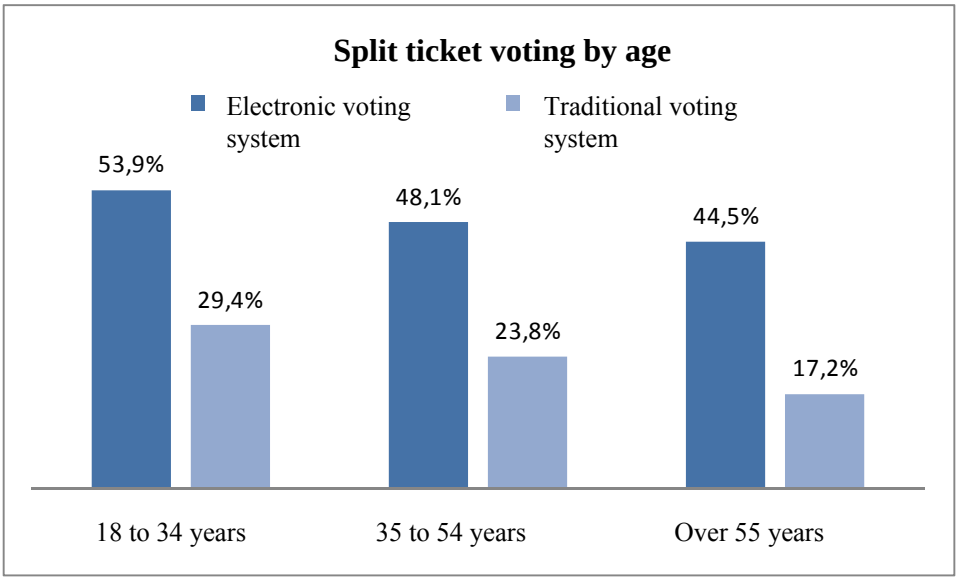



Fig. 2: Percentage of split-ticket voters using and their voting methods, broken down by age "Which voting method of voting did you use in today´s election?", Source: survey of 1502 voters

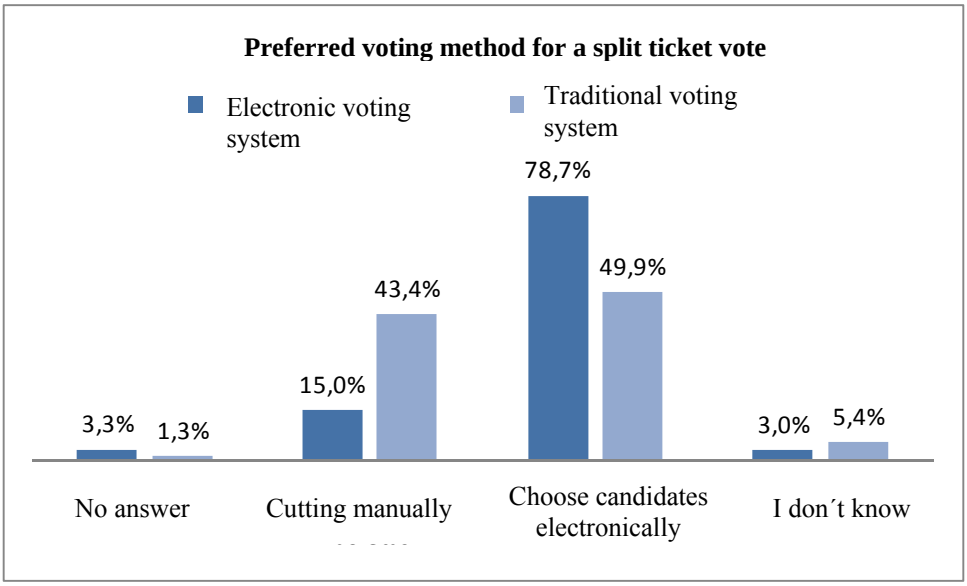



Fig. 3: Preferred method for voting a split ticket. "If you wish to vote for candidates of different parties, which voting method do you prefer?
Source: survey of 1502 voters

## 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].

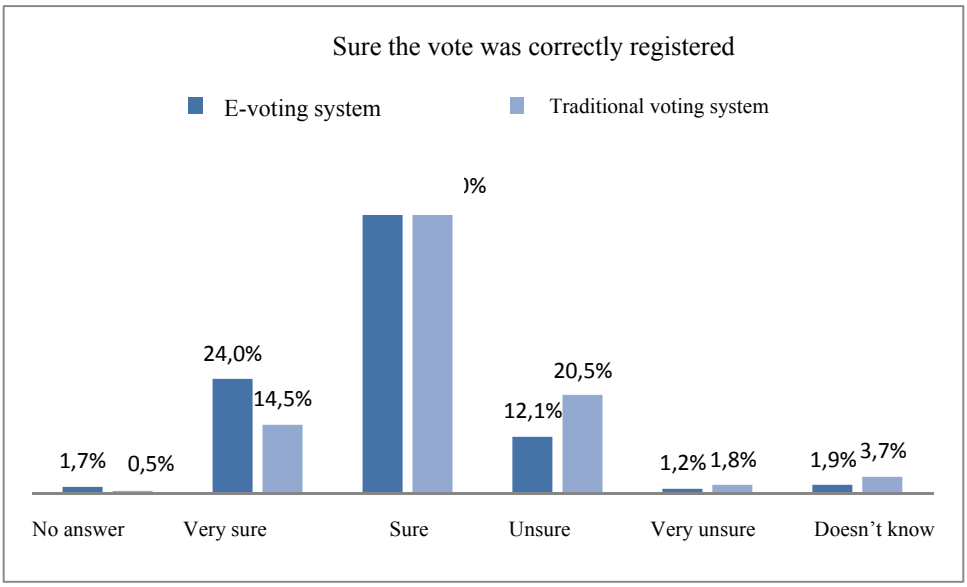



Fig. 4: Answers to questions "Are you sure your vote was correctly registered?
By voting system, Source: survey to 1502 voters

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.

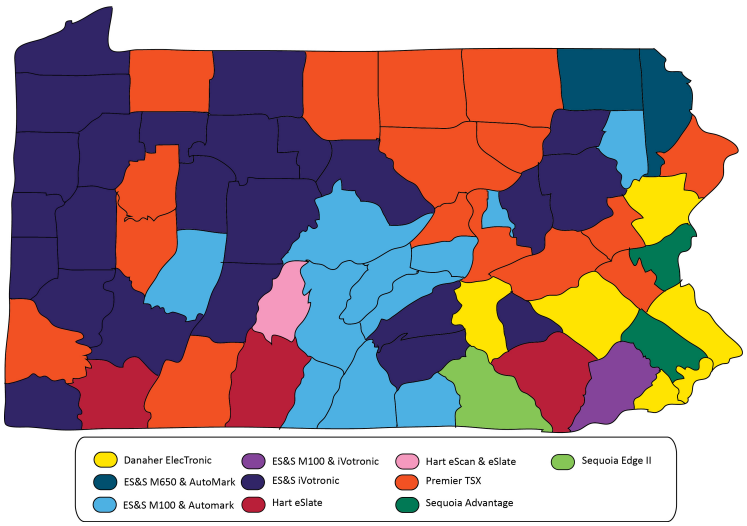



Fig. 1: Voting systems in Pennsylvania, 2008

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.

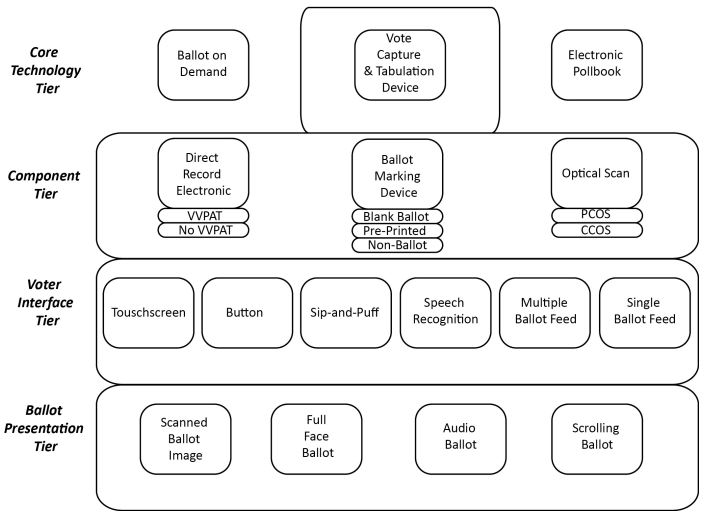



Fig. 2: Electronic Voting Classification Structure

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<br><br>- Long-term secrecy: for the same reasons as in Austria's case | + User-friendliness: for the same reasons as in Austria's case<br><br>- Ease of use: the voter has to enter two PINs | + Cost for smart cards: for the same reasons as in Austria's case<br><br>- 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<br><br>- 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<br><br>- 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<br><br>- 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<br><br>+ 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<br><br>- 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 $i \in \mathbb{Z}\{j,k\}$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 $Pr|guess = pv| - \frac{1}{2} \leq \epsilon$ „ $\epsilon$ 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.

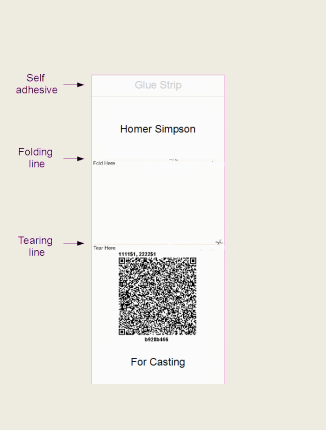



Fig. 1: Dual-ballot before folding. Since it is for casting, there is no barcode in the lower part of the ballot


Fig. 2: Audit ballot. The audit information is printed in the barcode in the lowest part of the ballot

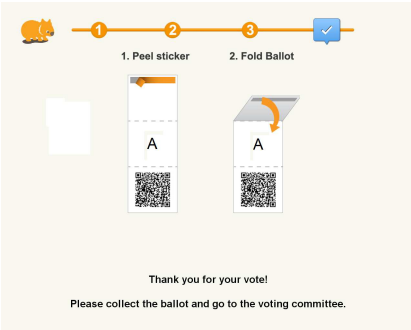



Fig. 3: Folding a ballot

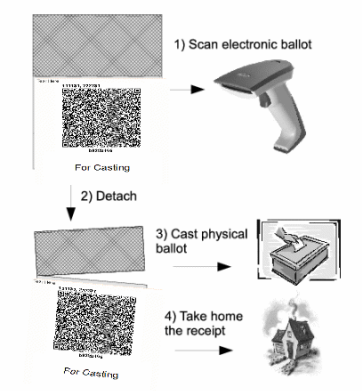



Fig. 4: Casting

### 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.

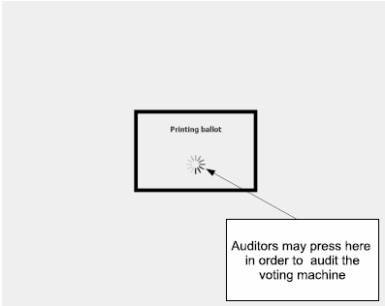



Fig. 5: Screenshots of the printing window with the hidden audit button

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 $\pi_c$ 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 $\pi_c$ 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.