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

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

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

The volumes are published in German or English

Information: http://www.gi-ev.de/service/publikationen/lni/

Robert Krimmer (Ed.): Electronic Voting 2006

GI-Edition

Lecture Notes in Informatics

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2nd to 4th of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.

P-86

Proceedings

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe,
ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

Gesellschaft für Informatik 2006

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

Volume P-86

ISBN 978-3-88579-180-3
ISSN 1617-5468

Volume Editor
Mag. Robert Krimmer
E-Voting.CC
Competence Center for Electronic Participation and Electronic Voting
Liechtensteinstrasse 143/3
A-1090 Vienna, Austria
Email: r.krimmer@e-voting.cc

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

It is now two years since we last met at Castle Hofen to discuss important topics involved with electronic voting. Back then it was intended to bring together interested people in e-voting. What was first planned as a sole academic meeting in the field of information technology has fast become a get-to-gether of academia, administration and vendors in the field. This is for sure due to the high level of interdisciplinary and high interest on all sides.

Two years ago we listened to the presentation of the Council of Europe recommendation on legal, technical and organisational on electronic voting or many other ambitious plans on implementing electronic voting.

Looking at this year's contributions we can easily see the fast development the field has undertaken. First of all thanks to the support of the Council of Europe our meeting serves as an academic review meeting for the back then discussed recommendation. Second we also have first empirical data on the actual use of e-voting in legally binding political elections and deal with so important topics like the observation of electronic voting. It is also good to see that the discussion on electronic voting is becoming a global one. While in 2004 the attendees of the workshop came from 11 countries, this year we have participants coming from nearly 30 different countries as far away like New Zealand or Brazil.

For our call of papers we received over 40 submissions of which we had to select the 20 best for presentation. This was done in a double-blind review process which wouldn't have been possible without the tremendous effort the programme committee members and the additional reviewers put in the process.

Special thanks go to the Council of Europe for their support in organizing this conference. I wish to thank Simon French, Wolfgang Polasek, David Rios, and Simon French as well as the remaining members of the TED steering committee for supporting once more our workshop.

Further thanks go to the German Society of Informatics and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Computer Society, the Federal Computing Centre for their continued support.

Without the help of the programme committee, especially Nadja Braun and Thomas Buchsbaum, who were always available with their advice that helped shaping the workshop the way it is today.

Finally I would like to thank Terry Davis general secretary of the Council of Europe and Jürgen Weiss vice chairman of the Austrian Federal Council that the conference can take place under their auspices.

Vienna, August 2006 Robert Krimmer

Programme Committee

- Frank Bannister, Ireland
- Nadja Braun, Switzerland
- Thomas Buchsbaum, Austria
- Tony Cresswell, USA
- Rüdiger Grimm, Germany
- Marjin Janssen, The Netherlands
- Simon French, United Kingdom
- Robert Krimmer, Austria (Chairman)
- Hannu Nurmi, Finland
- Wolfgang Polasek, Switzerland
- Alexander Prosser, Austria
- David Rios, Spain
- Fabrizio Ruggeri, Italy
- Daniel Tokaji, USA
- Melanie Volkamer, Germany
- Maria Wimmer, Germany

Additional Reviewers

- Bernard van Acker, Belgium
- Daniel Brändli, Switzerland
- Craig Burton, Australia
- Fiorella De Cindio, Italy
- Astrid Dickinger, Austria
- Sonja Hof, Switzerland
- Jason Kitkat, United Kingdom
- Nico Lange, Finland
- Herbert Leitold, Austria
- Margaret McGaley, Ireland
- Anne-Marie Oostveen, Netherlands
- Jordi Puiggali, Spain
- Peter Reichstädter, Austria
- Michael Remmert, France
- Thomas Roessler, Austria
- Ronald Vogt, Germany
- Peter Wolf, Bosnia and Herzegovina

Organizing Committee

- Friederike Findler, Austria
- Sandra Huber, Austria
- Ilse Klanner, Austria
- Katharina Kozlik, Austria (Chairman)
- Wolf-Heinrich Reuter, Austria
- Stefan Triessnig, Austria

Sponsors

OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

BUNDESRECHENZENTRUM BRZ

Co-Organizers

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

EUROPEAN SCIENCE FOUNDATION ESF

ifip

e-voting.cc

Webcast

All presentations are available in Audio & Video including slides at
http://www.e-voting.cc/2006 with the help of

WWW.monitorTV.AT
DER IT- UND BUSINESS-TV-CHANNEL

VORARLBERG ONLINE

Content

Overview

Robert Krimmer

E-Voting.CC
Competence Center for Electronic Participation and Electronic Voting
Liechtensteinstrasse 143/3
A-1090 Vienna, Austria
r.krimmer@e-voting.cc

Although the recent developments might give the impression that e-voting is an invention of the last decades, in fact it was one of the first applications of computers in public environments. First voting machines even date back to the end of the 19th century. The idea of modernising elections through electronic means has been an issue of visionary people early on. Forward thinkers like Fromm, Fuller, Arterton or Rheingold [From55, Full63, Arte87, Rhei93] have come up with ideas on how electronic voting could change and enhance democracy as such.

In the past years many governments have started to adopt computer-supported applications for their administrative processes; applications range from the simple download of forms to Internet-based submission of applications. Amongst these the most controversial application is electronic voting, which stands for the use of electronic means in elections. Motives for implementing electronic voting procedures are manifold, amongst the most important are as noted in the 2004 Council of Europe recommendation for electronic voting [CoE04, Remm04]:

1. enabling mobility of the voters
2. facilitating the participation in elections from abroad
3. raising voter turnout by offering additional channels
4. widening access for citizens with disabilities
5. reducing cost
6. delivering voting results reliably and more quickly

While the first four are benefits for citizens in the field comfort and participation and last two are benefits for administrators in the field of process workflows and costs. Also the last two are benefits that hold for any form of e-voting while the first four are mainly to be found for remote electronic voting. This might explain part of the controversies with citizens involved with electronic voting machines. In transition democracies the last two reasons are especially important as they promise to solve on one hand problems with alphabetisation of the population and problems with infrastructure in regard to delivering the results in time.

Therefore electronic voting not only serves as aid in counting the votes, by now they support all three main voting processes:

1. Pre-Election Phase: Identification of the voter, checking of eligibility
2. Election Phase: Casting the vote
3. Post-Election Phase: Counting of the votes.

Besides the discussion of polling place e-voting the debate in many countries specially concentrates on remote electronic voting, i.e. through the Internet and shares the common problems of remote voting procedures like vote coercion and buying.

<table>
<tr><th>Environment
Medium</th><th>Controlled</th><th>Uncontrolled</th><th></th></tr>
<tr><td>Paper</td><td>Polling Place</td><td>Postal Voting</td><td rowspan="3">Counting Machines</td></tr>
<tr><td rowspan="2">Electronic</td><td>Stand-Alone
Electronic Voting Machine</td><td rowspan="2">Remote
Electronic Voting
(PC, Cell Phone)</td></tr>
<tr><td>Networked Electronic
Voting Machine</td></tr>
<tr><td></td><td colspan="2">Networked Kiosk Electronic Voting</td><td></td></tr>
</table>

Figure 1: Forms of Voting [cp. VoKr06]

In general electronic voting is based on the separation of voter identification and vote casting as identified by Nurmi [NSS91]. Basic technologies for identifying voters are [VoKr06]:

- Username and passwords [knowledge]
- Transaction Numbers (TAN) [possession]
- Smart Cards [possession and knowledge]
- Biometric properties [might also be combined with the above].

For anonymity purposes these are [VoKr06]:

- Organisational pre-registration [handing out TANs]
- Hidden result calculation [using hardware security modules]
- Blind signatures

While the worldwide implementation approaches might be different in detail, many efforts still share the criticism by the public in regard to the lack of transparency of the application itself. Oostveen and van den Besselaar have shown that trust in the e-voting process is not dependent on the actual level of security but on the user's belief how secure the system is. This belief is largely dependent on the transparency of a system and here the 'main challenge for electronic voting [comes in:] the lack of transparency' [OoBe05].

The programme committee therefore tried to select the best papers based on their relevance to the conference topics and their quality to contribute to the growing need in qualified and argued discussion of the emerging topic of e-voting. The papers are grouped in nine sessions, which address the topics of experiences made with e-voting, social, technical, political issues as well as legal and democratic issues of e-voting, analyzing solutions for the uncontrolled environment, redesigning workflows for e-voting, observation, implementation and security of e-voting and finally political views and democratic challenges.

In session one the first hands-on experiences with legally binding political elections are presented. It includes two papers with reports from Estonia and Switzerland. *Ülle Madise* and *Tarvi Martens* explain the technological and legal point of view in Estonia as well as empirical findings on who were the voters in the worldwide first country-wide binding internet e-voting. *Nadja Braun* and *Daniel Brändli* then evaluate the swiss e-voting pilot projects and depict a road ahead for the time after the first trials.

The second session then tries to give an interdisciplinary view on the topic by looking at deep technological advances, political issues and social implications. It starts with a paper by *Ana Gómez*, *Sergio Sánchez Garcia*, and *Emilia Pérez Belleboni* who present an advanced technological solution based on a java card for future enhancement of smart cards to best suit electronic voting. In the second paper *Jordi Barrat Esteve* tries to answer the questions do we really need electronic voting and in which way (not) to take to implement it. *Laurence Monnoyer-Smith* then brings up the topic of the change of the voting ritual. This discussion is very necessary as the experiences in Ireland have shown us.

Session three addresses the legal and democratic issues of e-voting. *Rosa M. Fernández*, *Esther González*, and *José Manuel Vera* present the legal regulations set for e-voting in the autonomous Spanish Basque community. The experiences with e-voting in Brazil are presented by *José Rodrigues-Filho*, *Cynthia J. Alexander*, and *Luciano C. Batista*. They give a report about how e-voting have unwished results when implemented in the wrong way.

In the forth session we analyze how possible influence on the voter can be handled in the uncontrolled environment. *Melanie Volkamer* and *Rüdiger Grimm* first discuss the possibility of multiple casting a vote. *Gerhard Skagestein*, *Are Vegard Haug*, *Einar Nødtvedt*, and *Judith Rossebø* then conclude with an architecture for trust building measures in the uncontrolled environment.

The topic of the fifth session is the election process and to support and redesign it. *Alexandros Xenakis* and *Ann Macintosh* present an methodology on how to re-engineer an electoral process to make it fit for e-voting. *Goran Obradovic*, *James Hoover*, *Nick Ikonomakis* and *John Poulos* then present their solution for a fully supported electronically supported election workflow.

Session six's topic is observing and testing of electronic voting. *João Falcão e Cunha*, *Mário Jorge Leitão*, *João Pascoal Faria*, *Miguel Pimenta Monteiro*, and *Maria Antónia Carravilla* present their methodology used to test e-voting systems used for Portuguese parliamentary elections. The election specialist *Kåre Vollan* presents the problems of to observing electronic voting. *Jörn Schweisgut* then concludes with a technical solution to allow for observers in e-voting and solve the problem of voter coercion.

The implementation of e-voting is discussed in session seven. *Carol Boughton* presents the eVACS system and how it maintains the democratic values. Letizia Caporusso, *Carlo Buzzi*, *Giolo Fele*, *Pierangelo Peri*, and *Francesca Sartori* presents results of an implementation process of an Italian e-voting project and propose a careful approach.

The session on security for e-voting is the eighth. In an collaboration effort *Rüdiger Grimm*, *Robert Krimmer*, *Nils Meissner*, *Kai Reinhard*, *Melanie Volkamer* and *Marcel Weinand* present the approach of the Gesellschaft für Informatik on how to develop a protection profile. *Klaus Diehl* and *Sonja Weddeling* then present how their system is guaranteeing the German election principles.

The last session then gives room to democratic challenges and the politician's view on e-voting. *Joan Josep Piles*, *José Ruiz*, and *José Maria Moreno-Jiménez* present the challenges their e-voting proposal for what they call the e-cognocracy. Finally *Tina Jukić* and *Mirko Vintar* bring the often forgotten politicians on the table and present their view that might give answers to some questions we raised before.

As you can see this proceedings volume gives a heterogeneous picture of what is state of the art and what are current topics of discussion in the e-voting community. This gives good hope for a successful continuation of our e-voting workshop at Castle Hofen in Austria. For the future it will also be interesting to develop a road map of future research which would then guide the development and implementation of e-voting worldwide.

References

[Arte87] Arterton, C.: Teledemocracy: can technology protect democracy? Sage Publications, Newbury Park, Washington D.C, 1987.

[CoE04] Council of Europe (2004): Electronic Governance. Recommendation Rec(2004)15 and explanatory memorandum, Council of Europe, Strassbourg, 42 pages.

[From55] Fromm, E: The Sance Society. New York, Rinehart, 1955.

[Full63] Fuller, B. R.: No more Secondhand God, Southern Illinois University Press, 1963.

[OoBe05] Oostveen, A., van den Besselaar, P.: Trust, Identity, and the Effects of Voting Technologies on Voting Behavior, Social Science Computer Review (23) 3, 2005, pp. 304-311

[Remm04] Remmert, M.: Towards European Standards on Electronic Voting. In: Prosser, A., Krimmer, R.: Proceedings of the 1st ESF TED Workshop on Electronic Voting, GI LNI P-47, Bregenz, 2004, pp. 13-16.

[Rhei93] Rheingold, H.: The Virtual Community, Addison-Wesley, Reading, 312 pages, 1993.

[VoKr06] Volkamer, M., Krimmer, R.: Die Online-Wahl auf dem Weg zum Durchbruch. Informatik Spektrum, Springer,

Session 1: E-Voting Experiences

E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world

Ülle Madise[1,2], **Tarvi Martens**[1]

[1] National Electoral Committee
[2] Tallinn University of Technology
Lossi plats 1 a
15165 Tallinn Estonia
ylle.madise@riigikontroll.ee
tarvi@sk.ee

Abstract: At Estonian local elections in October 2005 for the first time in the world binding country-wide remote Internet voting took place: whole Estonian electorate had a possibility to cast the vote via Internet. Approximately 2 % of actual voters made use of this possibility. The e-voting surveys show that the attitude of the Estonian public toward e-voting was and is positive; gender, income, education, type of settlement and even age are no important factors by choosing e-voting from all voting channels; the use of e-voting possibility depends mostly on the trust in the procedure of e-voting and E-voting in itself does not produce any political effects. Estonian e-voting experience in 2005 reassures the hypothesis that e-voting does not raise the voting activity of people who never take part in elections, but it can encourage the participation of voters who vote sometimes. Thus, e-voting could slow down the trend of falling participation. Despite successful e-voting experience in October 2005, the political debate around e-voting has started in Riigikogu (Estonian Parliament) again. If the e-voting provisions will not be excluded from the law, the next country-wide e-voting in Estonia is taking place February-March 2007 by next Riigikogu elections.

1 Background

Estonia is widely credited to be a pioneer in e-governance and e-democracy. The use of digital channels for different services is steadily widening, nearly half of households have a computer at home and more than 4/5 of those are connected to the Internet. There are 55 public Internet access points per 100 000 inhabitants and all schools are connected to the Internet. Estonia is the only country in the world, where ID card with remote identification and binding digital signature functions is compulsory whereby ~70 % of Estonian inhabitants are already cardholders.[1] Therefore introducing e-voting[2] was a logical step to take and e-voting could be seen as an essential convenience in an information society, like using Internet for sending tax declaration etc.

The declared aim of the launching of online voting was to increase voter turnout and fight against political alienation. The participation rate at local government council elections in Estonia is usually ~ 50 % and at parliamentary elections ~ 10 % higher. The voter turnout did not exceed 70 % even at the constitutional referendum in 1992. So, the problem of low turnout really exists in Estonia. Since especially young voters' turnout is expected to rise, the most active supporters of e-voting are those parties, who hope to gain additional votes from an increased turnout. The angriest opponents seem to be those parties, who would probably lose their position in respective representative bodies that are composed on the principle of proportionality.

2 Theoretical fears and threats

The political agreement to introduce e-voting in Estonia beginning at 2005 elections was made in 2002[3]. In the discussion about introduction of e-voting classical arguments about conformity of the e-voting with the principles of fair elections incl reliability of electronic voting systems were changed, whereby one of typical arguments against e-voting was that people who have no commitment to go to the polling station to execute their citizen's duty, should not participate in governing at all, which attitude contradicts to the axiom that the higher the turnout is the better. The threats and fears around e-voting can be divided into two major groups:

- Purely political fears: some parties are afraid that the possibility to e-vote brings some people to vote, who otherwise would not participate. If those, who otherwise would not participate, would vote, the position of those parties, whose supporters prefer traditional voting in the polling station (or if said directly: who are ready to go to the polling station), could worsen. This fear is based on the assumption that possible e-votes are not divided proportionally between the parties;

---

[1] See the ID-card webpage in English: http://www.id.ee/pages.php/030301 [accessed on 01-05-2006].
[2] The public in Estonia is used to the meaning of e-voting explictely as Internet voting: other means of the electronic voting like a punch-card, optical scan ballot etc have never been seriously considered, therefore not known by the public. So the use of the notion "i-voting" would cause confusion.
[3] See about the genesis of the Estonian e-voting project in: [DM04]

- Possible lack of legitimacy of the election results because of following:

    - The individual e-voting procedure can not be supervised by authorities or observed in a traditional way, therefore massive buying and selling of the votes as well exercise of other influence or pressure on the voter are possible;

    - E-voting results can not be verified by the people themselves, and people need to have an absolute faith in the accuracy, honesty and security of the whole electoral apparatus (people, software, hardware). Thus, for people who didn't program the system, the operations of the computers can truly be verified only by knowing the input and comparing the expected output with the actual outcome. Under a secret ballot system, there is no known input, nor is there any expected output with which to compare electoral results.

Certainly it is important to realize, that legitimacy of e-voting or the elections results in whole can be challenged for purely political or personal reasons by some politicians, cryptographs or other opinion leaders without any objective cause.

2.1 Technological point of view

Risks of e-voting must be analyzed from different viewpoints, starting from the general public level and proceeding to more technical issues. There are a large variety of risks on each level; in this paper we will focus on the most principal and important ones. From the general public viewpoint, the major risks of e-voting include the following:

- Incorrectness or untrustworthiness of the voting results, which remain unnoticed at the time of elections (for example, voters are illegitimately influenced, multiple votes from one person are counted, a wrong vote is counted and so on).

- Breach of the voter's anonymity (for example, a person's political preferences will be presented to the general public).

- Annulment of the elections, interruption of the voting process (for example, due to a major security breach in e-voting).

From these three risks, the first two are the most serious. Annulment of the elections may be expensive, but tends to be politically less sensitive.

On the technical level these major risks are especially critical due to three principal problems of e-voting. Historically, one of the primary arguments has been that the security requirements of e-voting are extremely difficult to satisfy due to the conflicting requirements of confidentiality and auditability. The confidentiality requirement states that votes must remain anonymous; the auditability requirement - that every action in the system must be recorded.

A major argument against Internet e-voting states that Internet is an inherently insecure platform. Indeed, various attacks including worms, viruses, spy ware, spoofing, denial of service and others, can be used to compromise the voting results, to break the voter's anonymity, or to interrupt the elections. The vulnerabilities behind these attacks arise from the fundamental properties of the architecture of Internet and current personal computers. It has also been noted that (seemingly) successful e-voting trials do not really prove security of Internet voting. First, it is very difficult to prove that no security breach has occurred; and second, successful trials cannot eliminate security risks for future elections.

Finally, due to these and other problems the e-voting is sometimes argued to be not cost-effective: security measures complicate the election process and the small number of e-voters does not justify the additional costs resulting from this complexity.

2.1 Legal point of view

According to the Estonian Constitution members of the *Riigikogu* as well local government councils shall be elected in free elections based on the principle of proportionality, elections shall be general, equal and direct, and voting shall be secret. There is no special regulation for e-voting in the constitution. It is absolutely clear, that remote Internet voting makes it impossible, to guarantee privacy by the voting act. On the other hand, the required principle of uniformity gives rise to questions about equal access to participate in the voting process and additionally general equality issues.

3 Experience

3.1 Legal solutions

The principle of secrecy consists of the sub-principle of privacy and anonymity (secrecy of the election decision). Remote Internet voting requires in the first line rethinking of the principle of privacy. Voting in privacy should not be regarded as an aim by itself. The principle of secrecy, and its sub-principle of privacy, is there to protect an individual from any pressure or influence against her or his free expression of political preference. So it is a mean for guaranteeing freedom of choice. Such teleological approach to the constitution was the basis of the e-voting provisions from the very beginning of the whole project. [DM02] If we can not use compulsory privacy for guaranteeing the principle of freedom to vote, we must find an another method. The Estonian election law gives the e-voter the right to alter the vote given by electronic means with another e-vote or paper-ballot whereby the paper-ballot has priority. So a “virtual polling booth” is created: the e-voter can choose the moment, when she or he is alone, free of any possible pressure. On the other hand it is an efficient instrument against purchasing of votes. The e-voters possibility to change their e-vote reduces the motivation to exercise any influence or pressure including offer money or goods for any votes.

In Estonia, other that in some countries, the fact whether a person entitled to vote did participate in voting or not, is not regarded as a part of the principle of secrecy. The voter lists that contain information about participation and chosen voting method are preserved in the archive and can be used for research purposes. Researchers have made use of this possibility; incl for the e-voting survey, what unfortunately weakened somewhat the public trust against e-voting. The fact that the official questioner had knowledge about the actual fact of e-voting made some people suspect about the secrecy of their voting decision. These suspicions were leaked in public media but they were more or less kept unmarked. The explanation was that voters' lists have always had according information about who participated and what voting method was used. The voting decision itself has always been secret.

Some months before the municipal elections 2005 the President of Estonia brought e-voting provisions to the Supreme Court for constitutional review arguing that the possibility to change e-votes gives advantages to e-voters in comparison to non-e-voters. E-voters can change their vote for an unlimited number of times but only during e-voting and advance poll days (from sixth to fourth day before actual voting day, i.e. from Monday to Wednesday). The initial version of the e-voting law contained the possibility to change the e-vote with a paper-ballot on the actual voting day. This provision was left out of the law, because this could have given real advantage to e-voters: they would have had the chance to change their election preference on Sunday after receiving additional information about candidates in the second half of the week. After this change all voters who use advance poll possibilities are formally in the same conditions.

The Supreme Court Chamber of Constitutional Review pointed out that despite the repeated electronic voting the voter has no possibility to affect the voting results to a greater degree than those voters who use other voting methods. From the point of view of the voting results this vote is in no way more influential than the votes given by paper ballot. According to the Estonian Election law[4] each voter shall have one vote. When a voter has given several votes electronically, the last vote shall be taken into account. If a voter has voted both electronically and by a ballot paper, the ballot paper shall be taken into account. Within the system of electronic voting the taking only one vote per voter into account is guaranteed by a system similar to the so called system of two envelopes, used upon voting outside the polling station of one's residence during advance poll days.

Upon voting by electronic means a voter makes her or his choice, which shall be encoded (placed in a so-called virtual inner envelope). Thereafter the voter shall approve the choice by his or her digital signature, which means that personal data is added to the encoded vote (so-called outer envelope). The personal data and the encoded vote shall be stored together until the counting of votes on the Election Day, with the aim of ascertaining that the person has given only one vote.

[4] See the e-voting provisions in [MVM06]

The personal data of a voter and the vote given by the voter shall be separated after the fact that the voter has given only one vote has been checked and repeated votes have been eliminated. It is possible to open the so-called inner envelope only after the personal data added to the encoded vote have been separated with the help of a key given only to the members of the National Electoral Committee, after the polling stations have been closed. Thus, the system of electronic voting guarantees that only one vote per voter shall be taken into account, ensuring, at the same time, that the voting decision remains secret.

Pursuant to the petition of the President the violation of uniformity of voting also consists of the fact that through the possibility to change the e-vote given for unlimited number of times gives advantage to the e-voters in comparison to other voters; That because other voters do not have the possibility to change their vote. The Chamber said that this interpretation renders the principle of uniform elections a special case of general right to equality. In the legal sense e-voting is equally accessible to all voters. The ID-card necessary for e-voting is mandatory for all inhabitants of Estonia, thus, the state has created no legal obstacles to anyone to e-voting, including to changing one's vote during the advance poll days. It is a fact, that due to factual inequality the possibility to change one's vote through e-voting is not accessible to all voters can be regarded as an infringement of the general right to equality and the principle of uniformity. The principle of equal treatment in the context of electing representative bodies does not mean that absolutely equal possibilities for performing the voting act in equal manner should be guaranteed to all persons entitled to vote. In fact those who use different voting methods provided by law[5] are in different situations. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the Constitution. The aim to increase voter turnout is without any doubt legitimate. The measures the state takes for ensuring the possibility to vote for as many voters as possible are justified and advisable. Another aim of allowing e-voting is the modernization of voting practices what coincides with the aims of e-voting listed in the Recommendation (2004)11 "Legal, operational and technical standards for e-voting" of the Council of Europe.

In accordance with the Penal Code, preventing a person to freely exercise his or her right to elect or be elected at an election or to vote at a referendum, if such prevention involves violence, deceit or threat or takes advantage of a service, economic or other dependent relationship of the person with the offender is punishable by a pecuniary punishment or up to one year of imprisonment. The voter's possibility to change the vote given by electronic means, during the advance polling days, constitutes an essential supplementary guarantee to the observance of the principle of free elections and secret voting upon voting by electronic means.

---

[5]The voting methods allowed in Estonia are: advance poll with paper ballot in- and outside of the polling station of voters' place of permanent residence from 13th to 4th day prior election day; postal voting from abroad; voting at the Estonian Embassies in foreign states; home voting on election day; voting in custodial institutions and hospitals; voting on an Estonian ship, electronic voting from 6th to 4th day before election day and voting with paper-ballot on election day. At local elections not all of them are allowed.

A voter who has been illegally influenced or watched in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again either electronically or by a ballot paper, after having been freed from the influences. In addition to the possibility of subsequently rectifying the vote given under influence, the possibility of voting again serves an important preventive function. When the law guarantees a voter, voting electronically, the possibility to change the vote given by electronic means, the motivation to influence him or her illegally decreases. There are no other equally effective measures, beside the possibility to change the vote given by electronic means, to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium. The infringement of the right to equality and of uniformity, which the possibility of e-voters to change their votes for unlimited number of times can be regarded as amounting to, is not sufficiently intensive to overweigh the aim of increasing the participation in elections and introducing new technological solutions.[6]

3.2 Did voters' turnout increase?

It is very difficult to measure, whether e-voting did influence actual participation rate. Analysis based on facts is impossible; the only way is to question voters and non-voters, especially e-voters whether they had cast their e-vote if the possibility to e-vote would not have existed. E-voting at local government council elections started on 10 October 2005 at 9 am and ended on 12 October 2005 at 8 pm on the web page www.valimised.ee. The e-voting turnout was ~2 % of actual voters, what was estimated as a good result. The research confirms that e-voting will probably not bring those people who principally do not participate to vote. If e-voting does increase turnout then only within those groups of voters, who sometimes vote and sometimes not.

According to the subjective estimation of participation in the absence of e-voting, 4,9% of the questioned e-voters gave the answer that they would certainly not have voted if e-voting would not have been offered; 13,6% gave the answer "probably would not have" [BT06]. According to the proportion of those, who vote in some elections or from time to time, among e-voters and voters at polling station, we see, that 29,2% of e-voters and 21,5% of voters voting at polling station belong to that group [BT06]. So, slight increase of turnout may still be possible. Postal voting is not allowed at local elections. Therefore it is possible, that some Estonian inhabitants living or working in foreign countries could have cast their vote only because e-voting was offered. According factual data unfortunately does not exist.

[6] Decision Nr 3-4-1-13-05 from 1. September 2005 of the Chamber of Constitutional Review of the Estonian Supreme Court. Resume in English in: [MVM06]

The number of persons eligible to vote	1.059.292
The number of votes:	502.479
Valid (incl e-votes)	496.345
Invalid	6.134
Turnout	47%
Total number of e-votes	9.681
The number / of amended repeat e-votes (more than 1 vote per voter)	364
The number of e-voters	9.317
The number of e-votes eligible for counting	9.287
The number of annulled e-votes	30
The % of e-votes amongst all votes	1,87%
% of voters who voted during pre-voting days (incl e-voters)	12%
% of e-voters among all voters who voted during pre-voting days	7%
The number of voters who used ID-card electronically for the first time (for e-voting)	5.774
The % of those, who used ID card for the first time electronically among all e-voters	61%

Figure 1: General statistics of local government elections 2005
(data: National Electoral Committee)[7]

Most popular e-voting times were in the very beginning and in the very end of the e-voting period: in the morning at 9 and in the evening at 19 (probably at the time when people got to their workplace or in the evening at home). During the whole e-voting period, the number of e-voters was the largest at the beginning of the voting period and even larger during the very last hour of e-voting [MVM06]. Most e-votes were given at home (according to the survey 54,5 %); 36,6 % at workplace; 3,6 % at a friends place, cybercafé etc; 3,2 % at a public Internet access point and 1,9 % at the bank office [BT06]. The question, whether the fact that one's colleagues participate in e-voting does or doesn't motivate choosing e-voting or influence participation in general and whether it is good or bad for democracy, needs some further research.

	Women	**%**	**Men**	**%**
up to 29	1062	25,0	1512	30,0
30 - 34	542	12,8	908	18,0
35 - 39	506	11,9	688	13,6
40 - 44	497	11,7	553	11,0
45 - 49	451	10,6	433	8,6
50 - 54	362	8,5	345	6,8
55 - 59	278	6,5	228	4,5
over 60	547	12,9	375	7,4
TOTAL	**4245**	**100,0**	**5042**	**100,0**

Figure 2. Factual statistics about e-voters by age groups and gender

[7] More statistics at the National Electoral Committee web page: http://www.vvk.ee/english/results.pdf [accessed on 01-05-2006]

3.3 Non-discriminatory Access to the voting

The facts we do have, as well the results of surveys show that at the 2005 elections the problem of inequality in gaining representation because of e-voting did not exist. We are in the opinion that the digital gap increases social disparity in elections in today situation only if the number of voting stations decreases or the voting period will be abbreviated. Neither one nor another was the case by elections 2005. The principles of fair elections require formal equality of voting conditions, not material equality. It is generally impossible to guarantee strictly equal conditions for all voters: e.g. the polling station is for some people closer than to another. Therefore, the creation of new and more comfortable voting possibilities does not contradict to the constitutional principles of voting until we do not worsen the "old-fashioned" voting conditions. The most important reasons for not using e-voting were the absence of the Internet access and lack of computer knowledge (according to the survey 67,1 %). Approximately one-fifth of the questioned non-e-voters pointed out that a reason for not e-voting was the sufficiency of the paper-ballot system. Lack of trust with 3,2% and absurdity of e-voting with 1,9% were no dominant reasons [BT06]. Prior to the actual e-voting there was a concern that the possibility to change the e-vote is going to be misused. It was not the case. The general statistics shows that the number of amended e-votes was only 364 (see figure 1), including repeated votes given for demonstration by the members of the e-voting organizing-team. Gender is not an important factor when choosing e-voting from possible voting channels, age on the contrary is quite an important factor: most e-voters belong to the age group 18-29 (see figure 2). It is important to remark, that these age groups are not easily comparable: the age group of 18-29 is much bigger than the group of 30-34 etc.

The hypothesis that e-voting rewards advantages to urban electorate found no proof (see figure 3). When we look at the absolute number of e-voters by towns and rural municipalities, we can see that the largest number of e-votes was given in Estonian capital city Tallinn and in the second-large city Tartu. When we compare the percentage of e-votes with all votes cast in a municipality or town, it can be seen that at the top there is not Tallinn or Tartu but a tiny municipality, the island Ruhnu with 11.1%; neighboring municipalities of the capital city follow with ~4%. Tallinn ranks 15th and Tartu 29th, respectively with 2.75% and 2.42% of all votes. If we compare the percentage of towns and municipalities, the differences are not really great, with the exception of the county near the eastern border with Russian-speaking inhabitants. The exact reasons of e-voting turnout being so low in that area needs further research.

Among 240 districts, there were only 18 with no e-voters at all.

Type of settlement	**Type of political participation**			
	no vote	vote at polling station	e-vote	Total
Urban	67,9%	67,6%	70,2%	68,6%
Rural	32,1%	32,4%	29,8%	31,4%
Total *№ of respondents*	100,0% (305)	100,0% (318)	100,0% (315)	100,0% (938)

Figure 3. Frequency of Political Participation and Mode of Vote in 2005 [BT06]

3.4 Political effects

The initiator of the e-voting project *Reformierakond* (Reform Party) received the most e-votes (32,7 % of all e-votes; the percentage of e-votes in all votes given to Reform Party is 3,61), all other parties supporting e-voting did also well (respective percentages by Pro Patria 17,5 and 3,82; Res Publica 10,4 and 2,29; Social Democrats 9,9 and 2,86). Among other things the Reform Party organized ID-card user trainings and handed out complimentary smart-card readers during their election campaign. Parties who challenged the e-voting until the actual voting time *Keskerakond* (Center Party) and *Rahvaliit* (Peoples Union) received quite few e-votes (8,7 % of all e-votes; the percentage of e-votes in all votes given to Center Party is 0,63; respective percentages by Peoples Union 6,9 and 1,03). Important reason for that can be the opposition towards e-voting among their supporters. The Centre Party who on the background of their general success could have received many e-votes ranked only 5th among the political parties by the number of e-votes. [MVM06]

Prof A. Trechsel and F. Breuer assessed the possible political impact of e-voting using the results of the telephone survey and concluded political neutrality of e-voting (see figure 4).

Independent variables	**B**	**s.e.**	**sig.**
Age	0,267	0,116	0,022
Gender	0,415	0,287	0,148
Settlement	0,361	0,316	0,254
Education	0,289	0,181	0,111
Income	-0,166	0,136	0,221
Language	**-1,377**	**0,546**	**0,012**
Left-right scale	-0,008	0,073	0,908
Political discussions	0,270	0,162	0,095
Trust in Parliament/government	-0,265	0,342	0,438
Trust in politicians	0,188	0,316	0,551
Trust in the State	0,516	0,278	0,064
Computing knowledge	**-0,410**	**0,181**	**0,023**
Frequency of internet use	0,153	0,082	0,063
Location of internet access	0,247	0,172	0,150
Trust in transactions on the internet	-0,325	0,229	0,156
Trust in the procedure of e-voting	**-1,684**	**0,244**	**0,000**
Constant	1,004	1,723	0,560

Figure 4. Multi-variate global model of the impact of socio-demographic and –economic, political and ICT variables on choosing e-voting over voting at the polling stations (logistic regression coefficients). [BT06]

3.5 Technical and Organizational Measures used to ensure security and trustworthiness of e-voting

The organizational issues involve many different aspects. The overall organization of elections, including preparation of initial data, timing of e-voting, collection of results, handling (multiple) e-votes, and other, must support e-voting processes adequately. In spite of somewhat virtual character of the e-voting organization that may not be easy to define and protect from the information security viewpoint, its actors, roles, and responsibilities must be defined, assigned, and managed. In Estonian case, the organizational procedures, including risk management, security procedures, and security awareness activities, were be clearly defined. All e-voting procedures were identified; critical procedures that can lead to major risks were documented and audited by an accredited IT auditor.

The e-voting system was designed to deal with conflicting requirements of confidentiality and auditability. The concept of "digital double-envelope" was used [GD05]. According to it, e-voting should be in a sense analogous to voting with envelopes at a traditional voting (paper-ballot given outside home voting station of the voter and postal voting from abroad). Implementation of this concept may include representation of the inner envelope by an encrypted vote and the outer envelope - by a digital signature.

The e-voting system is managed on several levels: software development and modification, installation and initiation, the active e-voting and subsequent activities. Relevant risk management, configuration management, change management, contingency planning, disaster recovery planning, safeguard selection and implementation and follow up procedures were defined and implemented. System and network monitoring was performed by different parties on different levels during the e-voting period on a 24h basis. All major e-service providers (e.g. banks) and Internet operators were involved in the process with monitoring the overall “health” of Internet – network traffic loads, analysis of possible Trojans/viruses etc.

As of result – no serious attacks occurred and the system was stable. Counting of e-votes was a semi-open procedure with presence of more than 60 international observers, journalists, IT auditors and members of the National Electoral Committee.

4 Conclusion

Estonian e-voting experience seems to prove that it is possible to solve the legal as well technological obstacles. The compulsory ID card with remote identification and digital signature functions as well IT auditors as the guarantee of public trust play a crucial role in the successful experience. The system of e-voting has worked perfectly, all procedures have been legitimate and performed lawfully (respective confirmation of auditors is available).

The attitude to the e-voting of the Estonian public was and is positive[8]. There were no court cases and we do not have any information about purchase of e-votes (on the contrary to the votes on paper-ballot). Here we should underline again, that voting in privacy in the remote unsupervised Internet voting context is a right, not a duty.

The legality and legitimacy of the whole election process has not been questioned for political reasons. One of possible explanations for that can be the public debate about the concept of the Principles of Honest E-Voting[9], what should be certainly continued. The principles of uniformity and generality in their conjunction require that the participation in voting, guaranteed to voters, is as convenient as possible. New voting channels, incl. e-voting serve the aim of increasing the participation in voting and thus protecting the representative nature of representative bodies. E-voting does not change the voting behavior of those persons who principally do not vote in elections, but it accords participation opportunity to the people who have no time or commitment to go to the voting station. Due to several new comfortable voting methods incl. postal voting and advance poll the traditional significance of the Election Day as voting day is anyway gone.

Literature

[BT06] Breuer, F.; Trechsel, A.H. Report for the Council of Europe. E-voting in the 2005 local elections in Estonia. European University Institute. Project leaders Prof.Dr. Alexander H. Trechsel, European University Institute, Florence, Italy & Director of the e-Democracy Centre (e-DC), University of Geneva, Switzerland; Ivar Tallo, Director of the e-Governance Academy, Tallinn, Estonia. Florence, 06.03.2006.

[DM02] Drechsler, W.; Madise, Ü. E-voting in Estonia. – TRAMES 2002, 3, vol 6 (56/51).

[DM04] Drechsler, W.; Madise, Ü. "Electronic Voting in Estonia." In Norbert Kersting and Harald Baldersheim, eds. Electronic Voting and Democracy. A Comparative Analysis. Basingstoke: Palgrave Macmillan, 2004, p 97-108.

[MVM06] Madise, Ü.; Vinkel, P.; Maaten, E. Internet Voting at the Elections of Local Government Councils on 16 October 2005: Report. http://www.vvk.ee/english/report2006.pdf [accessed on 28.04.2006]

[GD05] Estonian e-voting system - General description http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf [accessed on 28.04.2006]

[8] Survey "e-voting and decreasing of political alienation". Faktum, December 2003;
Survey „The attitude of Estonian inhabitants toward e-voting", Faktum, February 2004;
Survey „The attitude of Estonian inhabitants toward e-voting", Faktum, February 2005;
E-voting Survey. Turu-uuringute AS, May - June 2005; Survey "Democracy and national interests". Faktum. October - November 2005.

[9] Available on the e-Governance Academy (eGA) web page: http://www.ega.ee/ [accessed on 28.04.2006]

Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed

Dr. Nadja Braun, Daniel Brändli[1]

Swiss Federal Chancellery
Political Rights Section
Bundeshaus West
3003 Bern, Switzerland
{nadja.braun | daniel.braendli}@bk.admin.ch

Abstract: In Switzerland the Federal Chancellery in cooperation with three cantons has carried out since 2003 a number of pilot trials with the aim of evaluating the feasibility of remote e-voting. Based on a legal basis respecting the council of europe's recommendations five pilot trials have been authorized at national referendums in 2004 and 2005. The pilot trials were evaluated for a number of different aspects, including the potential of e-voting to increase voter turnout, the security risks and its cost-effectiveness. The evaluation has shown that e-voting is feasible in Switzerland. The decision on how to proceed now rests with the Federal Council and the Parliament.

1 Introduction

At the request of the Federal Council and the Parliament and in cooperation with the cantons of Geneva, Neuenburg and Zürich, the Federal Chancellery has carried out a number of pilot trials over the last five years with the aim of evaluating the feasibility of e-voting in Switzerland[2].

In Switzerland, the terms "e-voting" or "vote électronique" are understood to refer primarily to so-called "remote e-voting"[3] – the casting of ones vote via the Internet, by SMS or by other electronic data transmission media. In direct-democratic Switzerland, e-voting is meant to include not only the casting of votes in elections and referendums, but ultimately also the giving of 'electronic signatures' for initiatives, referendums and proposals for candidates for membership of the National Council.

[1] The opinions expressed in this paper do not represent any official statement.
[2] The first milestone within this pilot phase was established by the report [B02] of 09.01.2002.
[3] The same procedure i.e. the casting of a vote elsewhere than in a polling station, is also referred to as "remote internet voting" or "remote voting by electronic means (RVEM)".

The pilot studies of recent years were restricted to voting in elections and referendums, as electronic signature might possibly require an officially recognized digital signature to enable positive identification of the signatory. To date, however, suitably approved digital signatures have not been sufficiently widely used in Switzerland[4].

The following two chapters give, firstly, an outline of the pilot studies and, secondly, a presentation of the major results of the evaluation[5].

2 Pilot Trials

2.1 Preconditions for pilot trials in Switzerland

The legal basis for the legally binding use of e-voting was created on 21st June 2002 within the context of a partial revision of the federal law of 17th December 1976 on political rights (BPR, SR 161.1)[6]. This legislation allows the Federal Council, in consultation with interested cantons and municipalities, to authorize pilot trials which are limited as to place, time and subject matter. A special requirement is that strict control of eligibility to vote, the secrecy of voting and the recording of all votes must be guaranteed. The trials must not be open to misuse. The rules of implementation (Art. 271-27q of the ordinance of 24th May 1978 on political rights, VPR, SR 161.11) set out the preconditions which must be fulfilled before the Federal Council can approve pilot trials of e-voting[7]. The rules of implementation likewise place special emphasis on ensuring security, protecting the secrecy of the vote, checking voter eligibility and preventing the casting of multiple votes.

In implementing the pilot projects, attention was also paid to the *recommendations of the Council of Europe*, in addition to the Swiss legal provisions [C04]. The core message of the CoE recommendation is that e-voting must respect all the principles of democratic voting, and must be as reliable and secure as non-electronic voting. In the recommendation, special emphasis is placed on there being a high level of security, on the characterization of e-voting as an additional form of voting and on the neutrality of the technology. These keynotes are fully endorsed in Switzerland.

---

[4] As of 1st January 2005 (Federal Law on electronic signature, ZertES, SR 943.03), the legal basis for binding transactions is in place.

[5] Publication of the evaluation in the form of a report of the Federal Council for the attention of the Parliament is planned for summer 2006.

[6] Art. 5 § 3, Clause 2, Art. 8*a,* Art. 12 § 3, Art. 38 § 5 and Art. 49 § 3 BPR plus Art. 1 § 1, Clause 2 Federal Law of 19.12.1975 on the political rights of Swiss living abroad (BPRAS, SR *161.5*).

[7] Cf. also the Federal Council directives to the cantons in the circular of 20.09.2002 regarding the application of these rules of implementation (Federal Gazette *2002* 6603-6609).

The *authorization of pilot projects* relating to national ballots is the responsibility of the Federal Council. In order to lessen risks, the Federal Council can limit the scope of the pilot project in respect of place, time and subject-matter. The conditions detailed in the Swiss ordinance on political rights must be observed cumulatively, unless the directive explicitly states otherwise. Any planned use of e-voting at the national level must be authorized in advance by the Federal Council. The cantons had to include detailed technical documentation in their requests for such authorization. Before the first trial, the three pilot systems were checked by professional outside companies engaged by the Federal Chancellery, to ensure that the systems were secure and hacker-proof.

An extremely important precondition for e-voting is the *standardization of the registers of voters*, which are normally kept by the communes. In developing their systems, the pilot cantons were able to refer in part to cantonal regulations, and in part to an agreed standard developed by the eCH association [E04, cf. also B05]. Individual cantonal or communal identifiers were used for personal identification in each case. Due to the lack of unambiguous numerical identification, no cross-cantonal exchange of data between the different voter registers was possible.

In order to preserve the secrecy of the vote, all personal data (name, address, date of birth etc.) were anonymized after the individual voting permits had been generated. The unique voting permit number could then be used to check (against the voting register) whether an individual had already voted, thus ruling out the possibility of multiple voting.

2.2 Pilot trials at national referendums in 2004 and 2005

In 2004 and 2005, a total of five e-voting pilot trials were carried out in the cantons of Geneva, Neuenburg and Zürich on the occasion of national referendums (cf. Table 1). Without exception, all five trials proceeded successfully and without mishap. Prior to the first official use, each of the three electronic voting systems was subjected to an extensive test run overseen by independent experts.

Date	Canton/Communes	Extent of trial	Number of electronic votes (share of all votes as %)
26.09.2004	Geneva: Anières, Carouge, Cologny, Meyrin	22.137 eligible voters	2.723 (21,8%)
28.11.2004	Geneva: Anières, Carouge, Cologny, Collonge-Bellerive, Meyrin, Onex, Vandoeuvres, Versoix	41.431 eligible voters	3.755 (22,4%)
25.09.2005	Neuenburg	1.732 eligible voters*	1.178 (68,0%)
27.11.2005	Zürich: Bertschikon, Bülach, Schlieren	16.726 eligible voters	1.154 (22,1%) (of which 243 by text message)
27.11.2005	Neuenburg	2.469 eligible voters*	1.345 (55,1%)

Table 1: Pilot trials carried out at national referendums

3 Evaluation of the Pilot Trials

The pilot trials were evaluated for a number of different aspects, including the potential of e-voting to increase voter turnout (3.1), the security risks (3.2) and its cost-effectiveness (3.3). These three aspects of the evaluation are summarized below.

3.1 Benefits to and effects on direct democracy

An important argument which is repeatedly raised in favor of e-voting is its potential to increase voter turnout. It is argued that certain groups – young people, on account of their increased use of the Internet; older people, because of their limited mobility; Swiss citizens living abroad, because of lengthy international mail delivery times; blind or partially-sighted persons – would make more frequent use of their voting rights if e-voting were in place.

* Users of the official "Guichet unique" electronic office

In 2004, the Federal Chancellery commissioned the research institute gfs.bern to undertake an empirical study on the potential effect of e-voting on voters across Switzerland [G05][8]. Two-thirds of the eligible voters currently have access to the Internet. The percentage is even higher for younger voters and those who are better educated. The survey revealed that 54% of those asked could imagine using e-voting. The most common reason given for readiness to use e-voting was its user-friendliness. Fears about data security were expressed most strongly by people who will probably not use e-voting.

"Assuming that you were already able to vote electronically, is it highly likely, very likely, fairly unlikely or highly unlikely that you would cast your vote electronically?"

© gfs.bern, Electronic Vote, 2003/2004 (N=4.018)

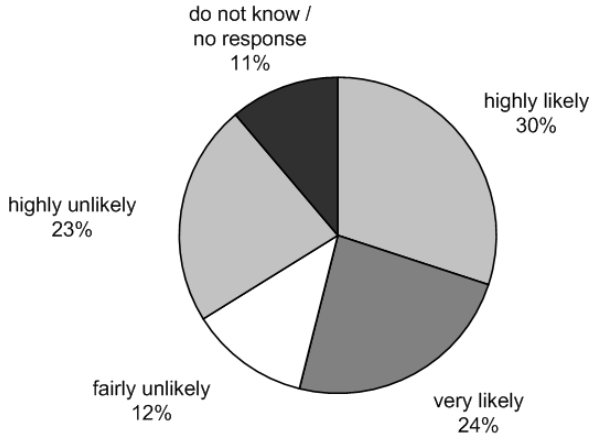

Figure 1: The potential effect of e-voting on Swiss voters

The use of e-voting was not only dependent on a person having available access to the Internet, but also on whether those asked make regular use of this medium for their professional and/or private affairs. Well-educated young males living in urban areas showed the greatest level of interest in e-voting. But the potential is greater than 50% even in the 40-65 age-group of voters and for people from the middle classes.

[8] The studies are based on a supplement to four VOX analyses (ex-post analyses of national referendums) from 2003 and 2004. A total of 4,018 Swiss citizens entitled to vote in national elections and referendums were asked for their opinion .

According to the study, e-voting is particularly attractive to people who stated that they did not vote in referendums either “at all” or “only sometimes”. This finding could be an indication either for a replacement by other forms of voting or for a potential increase in turnout. The potential is greater, the higher the level of interest in political issues and in active participation in political debate. Nonetheless, the study comes to the conclusion that e-voting would have no effect on the balance of power between the different political camps.

The Federal Council had as early as 2002 expressed some skepticism towards the estimates of certain experts of a possible increase in voter turnout [B02, p. 654f.]. Even after the completion of the pilot trials and their academic evaluation, it would be right to preserve such skepticism. The study cited here resulted in an unexpectedly high assessment of the potential of e-voting. As with the indications of a potential increase in voter turnout in all three pilot cantons, these findings would have to be corroborated by multiple trials in all three cantons.

3.2 Risks and security measures

Academics and scientists have grappled intensively with the risks of electronic voting, as e-voting has to meet the very highest security requirements [cf. e.g. A04; J04; M02; O02; R02; S04]. The emphasis has been on the dangers of technical manipulation, as well as on the general threat to a democracy posed by technical risks. Most fears concern ways of ensuring the secrecy of the vote [Br05; Mu02]. A major risk concerns the susceptibility to so-called ‘spoofing’. Voters could give their access data and their vote to a bogus Internet site without realizing it. Using the hacked information, unauthorized persons could subsequently submit their own political preferences to the official referendum server. A similar form of attack might consist in hacking unnoticed into the data flow between the official referendum server and the voter and changing the information so as to affect the vote (man-in-the-middle attack). Within company networks (Intranets), system administrators could try to spy on employees as they vote or seek to influence the vote in some way. It might be possible, finally, to use the buffer store of a voting machine to find out how an individual had voted.

Secure e-voting is feasible: the pilot trials have demonstrated this. But ongoing security depends on being able to maintain control of continually changing threats and risks. The necessary security measures cannot be developed and put in place once and for all. Just as the potential sources of danger (hackers, viruses, Trojan Horses etc.) are continually changing, so must the security measures be continually adapted and improved.

Many suitable security measures were tested as part of the pilot trials. It was important to rule out any risks of systematic misuse. As with conventional forms of voting (ballot-box or postal votes), the possibility that with e-voting, too, individual votes may be falsified, blocked or altered, or that a person’s voting behavior might be observed or deduced, can probably never be completely excluded. Everything must, however, be done to prevent the occurrence of any systematic irregularities or abuses [Br05].

The security measures taken during the pilot trials in the cantons of Geneva, Neuenburg and Zürich succeeded in foiling all registered attacks. Independent experts emphasized the efficiency of the security measures undertaken and credited each of the three cantonal systems with an excellent security architecture.

Postal voting is often used as a comparison to assess the risks of e-voting. Parliament demanded of e-voting a similar level of security to that of postal voting. The required benchmark was exceeded in the pilot trials. The following table[9] summarizes the requirements and the measures undertaken deriving from the legal and security considerations and compares them with analogous requirements and measures in respect of postal voting.

E-voting requirements	**Analogy(-ies) with postal voting**	**Measures taken during the pilot trials**
Positive identification: A person taking part in a referendum or an election must be positively identified as the person he/she claims to be.	Eligible voters give a handwritten signature on the voting permit or on the reply envelope. Voting slips are also filled out by hand.	• Individual and secret access code • Validation by indicating date of birth and/or place of birth • Use of digital signatures imaginable (in the future) • Other security queries such as the self-documenting AHV number would, however, be questionable (protection of secrecy of vote)
Authenticity of the e-voting system Voters must know for certain that their vote will be placed in the designated ballot-box and that it will be included in the count.	Postal votes are delivered by the postal service, handed in in person at the local authority office or posted in the community postbox.	• The SSL can be checked by the voter using his/her fingerprint • The authenticity of the server can be checked by means of a response code and/or pictorial symbols.
Single vote: A voter may cast only one vote.	The voting permit is issued only once and according to name. In postal voting, the original voting permit must be sent back in the return envelope. Repeat voting is thus impossible.	• Immediate cancellation of authorization to vote in the voter database, as soon as a vote (electronic or postal) has been registered • Clear signs on the voting envelope (e.g. an unbroken seal over the secret access code) show whether a citizen could have already voted electronically.
Preservation of voting secrecy/data protection: The voting intention of the voter must remain secret.	The completed voting slips reach the municipal offices in a separate sealed envelope. After verifying the signatures, the voting permit and the voting slip must be separated.	• Separate storage of personal data and voter-specific details on separate systems • Constant shuffling of the electronic ballot-box by means of a random generator. This makes it impossible, for example, to deduce the name of a person based on the sequence of votes cast.
Provisions against risks from 'Acts of God': Interference with voting from storms,	Analogous risks also exist for municipal offices/town halls, the special communal postbox, polling stations, postal sorting offices and	• Use of several redundant servers • Housing of servers in high-security buildings (entry control, fire protection, back-up power supply)

[9] The information in the table refers only to the solutions tested so far in Switzerland in the context of the pilot trials and does not claim to be exhaustive. Cf. also [V04, p. 57f.]

E-voting requirements	Analogy(-ies) with postal voting	Measures taken during the pilot trials
power failures, earthquakes etc.	postal delivery services.	
Reproducibility and provability: It must be possible to recount votes when the tally of votes is very close or in the event of an appeal.	Paper votes can always be recounted. Different people can be asked to undertake the recount. If they wish, citizens can be present at the recount (transparency).	• Preparation of conventional and electronic records, which are countersigned by the relevant authorities when the votes are counted • Preparation of a separate data storage medium (CD-ROM containing the data from the electronic ballot-box and all Log files) • The interests of voters are secured by special inspectors selected by the political parties
Trust: The entire procedure must be trustworthy and able to be checked.	Postal voting enjoys a wide measure of trust among the general public.	• Involvement of inspectors in all sensitive processes • Independent checking of the source codes, Open Source method • Disclosure of proprietary applications
Defence against external attack: a) Enduser devices (personal computers, mobile phones): possible interception and altering of the votes e.g. by the use of "Trojan horses".	Voting material is stolen from the eligible voter by removal from the letter-box after delivery. Systematic misuse cannot be excluded if many voters do not vote and do not tear up their voting papers before disposing of them.	• Multiple protection through Firewalls • Code-voting procedure (Zürich SMS, online transmission of the vote as a numerical code) • Use of state-of-the-art virus protection software
b) "Transport" of the vote from the user to the server: possible interception and alteration of the votes (man-in-the-middle attack).	Voting envelopes could fall into the wrong hands or be destroyed if they are removed from the communal postbox or if a postal sack is stolen or lost in transit.	• Encryption of the vote (SSL) • Details of vote transmitted graphically and not as text • All online packets are tested for their integrity using horizontal checksums
c) Platform (core element of an e-voting system): e.g. "Denial-of-service attacks"	Arson attack on the communal postbox. Or the delivery of the votes is impeded or prevented by a breakdown of the postal service. The risk is small, but increases with increasing centralization of postal services.	• Use of several redundant servers • Collaboration with various providers (DNS hacking)

Table 2: E-voting and postal voting: comparison of requirements and security measures

3.3 Cost-effectiveness of e-voting

Despite the need referred to above for e-voting to satisfy the highest security requirements, it must also be so simple to use that it can be used by every eligible voter. The challenge therefore lies in providing the greatest possible degree of security at an affordable price. At the same time, user-friendliness must not be excessively restricted. Postal voting can provide comparisons in this area too.

In its 2002 report, the Federal Council estimated the cost of a nationwide introduction of e-voting, including running costs over a 10-year period, at 400-620 million Swiss francs [B02, p. 685f.]. This summary estimate was reviewed using the data from the pilot trials. The Federal Chancellery tallied the total costs of the pilot projects at the end of 2005. There were also specific cantonal costs which were not borne by the Federal Chancellery (e.g. the cost of extra jobs and staff).

The financial cost for the development and operation of an e-voting system for both elections and referendums can amount to 15 million Swiss francs. The sum includes operating and maintenance costs for ten years, estimated staff and service costs and the amortization of the development costs. Such a system is scaled for a very large canton or for shared operation by several smaller cantons. If we assume that 1 million voters can use the system, the cost per electronic vote would be less than half a Swiss franc.

Assuming that several cantons operate an e-voting system together, and that those processes which are common to all forms of referendum (such as, for example, the printing of the voting permits, the creation of the voting register, the checking of voting rights etc.) feed into a cantonal or supra-cantonal election and referendum system, the implementation of e-voting would be more cost-effective than postal voting.

4 Conclusions

The pilot trials carried out at communal, cantonal and national levels have shown that e-voting is feasible in Switzerland. The pilot systems and the know-how gained by the pilot cantons is available to other interested cantons for the most part free of charge. The pilot cantons and some other cantons are interested in the progressive extension of the pilot trials to encompass the whole canton, and can also imagine extending the system to cover elections as well, if need be. This would require them to follow strategic guidelines laid out by the Federation, as well as federal assistance in the necessary adaptation of the existing legal provisions.

E-voting is a complex system involving many people at several different levels. A step-by-step approach makes it possible to gather experience and apply it to the improvement of electronic voting. Switzerland has approached the subject from the start at a cautious pace. Once the pilot phase was concluded, it was therefore possible to undertake a thorough evaluation of the various developments in the cantons and to point to a possible way forward. It is now for the political sphere to make the decisions as to how to approach the progressive implementation of an e-voting system. A cautious approach is also necessary in order to minimize risks. E-voting has only a chance of being introduced if all those involved – voters, politicians and authorities – have a lasting acceptance of and trust in the new procedures.

The decision on how to proceed now rests with the Federal Council and the Parliament.

References

[A04] Alvarez, R. Michael/Hall, Thad E.: Point, click and vote, Washington 2004.

[B02] Bericht über den Vote électronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte vom 9. Januar 2002 (report of 09.01.2002 on the Opportunities, Risks and Feasibility of the Electronic Exercise of Political Rights), Bundesblatt 2002, S. 645-700 (BBl 2002 645). Available at: www.admin.ch/ch/d/ff/2002/645.pdf.

[B05] Bundesamt für Statistik: Die Harmonisierung amtlicher Personenregister, kantonale und kommunale Einwohnerregister, Amtlicher Katalog der Merkmale (The standardization of official registers of persons, cantonal and communal registers of residents, Official Catalog of Criteria), Neuchâtel 2005. Available at: http://www.bfs.admin.ch/bfs/portal/de/index/infothek/erhebungen__quellen/statistik_und_register/registerharmonisierung/publikationen.Document.65357.html.

[Br05] Braun, Nadja: Stimmgeheimnis (Secrey of the vote), Diss. Bern 2005.

[C04] Council of Europe: Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies. Available at: http://www.coe.int/t/e/integrated_projects/democracy.

[E04] eCH-Standard "0027:Meldeprozesse" (Reporting processes), as of 29.10.2004. Available at: http://www.unisg.ch/org/idt/echweb.nsf/0/D38E4752D42D358AC1256F3C002F6B0A?OpenDocument&lang=de.

[G05] Research institute gfs.bern: "Das Potenzial der elektronischen Stimmabgabe" (The potential of e-voting), study commissioned by the Federal Chancellery, Bern 2005.

[J04] Jefferson, David/Rubin, Aviel D./Simons, Barbara/Wagner, David: Analyzing Internet Voting Security, Communications of the ACM, 47, Nr. 10, 2004, S. 59-64.

[M02] Mitchison, Neil: Protection against "internal" attacks on e-voting systems, in: Muralt Müller, Hanna/Auer, Andreas/Koller, Thomas (eds.): E-Voting. Tagung 2002 für Informatik und Recht, Bern 2003, S. 255-266 German and French only).

[Mu02] Muralt Müller, Hanna und Koller Thomas (eds.), E-Voting, Tagung 2002 für Informatikrecht, Bern 2002.

[O02] Oppliger, Rolf: E-Voting sicherheitstechnisch betrachtet, digma, 4, 2002, S. 184-188.

[R02] Rubin, Aviel D.: Security Considerations for Remote Electronic Voting, Communications of the ACM, 45, 12, 2002, S. 39-44.

[S04] Schryen, Guido: How Security Problems Can Compromise Remote Internet Voting Systems, in: Prosser, Alexander/Krimmer, Robert (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society, Bonn 2004, S. 121-131.

[V04] Der Vote électronique in der Pilotphase, Zwischenbericht der Bundeskanzlei vom 18. August 2004 (E-Voting in the Pilot Phase, interim report of the Federal Chancellery of 18.08.2004). Available at: http://www.admin.ch/ch/d/egov/ve/dokumente/Zwischenbericht.pdf).

Session 2: Social, Technical, and Political Issues of E-Voting

Contributions to traditional electronic voting systems in order to reinforce citizen confidence

Ana Gómez Oliva, Sergio Sánchez García, Emilia Pérez Belleboni

Dpto. de Ingeniería y Arquitecturas Telemáticas (DIATEL)
Universidad Politécnica de Madrid. Ctra. Valencia km. 7. 28031 Madrid. Spain
{agomez | sergio | belleboni}@diatel.upm.es

Abstract: This document provides a general description of the telematic voting scenario designed by the author's research group. This scenario reinforces verification procedures as key elements to achieve full acceptance of the system on the part of voters. To frame this work, a general overview of electronic voting is given and the conditions entailed by these systems are specified.

1 Problems inherent to telematic voting

Since the first experiments in the 1960's with computerized voting until today, in which electronic ballot boxes or Internet voting are being tested, the mass media highlighted a number of experiences around the world under the general concept of *electronic voting*. However, these experiments have involved diverse types of voting systems, where the security guarantees required in authentication processes, voting and tallying are provided in quite diverse forms. In [CGP02] the authors propose a classification of voting systems into several levels of complexity. We can therefore identify two main groups that are relevant to our work: i) Systems that substitute one of the physical components of traditional voting procedures with some type of electronic process (i.e. Direct-Recording Electronic), and ii) those that use telematic networks to link voters to a remote polling station. For the last several years, nearly all governmental action designed to automate voting processes involve policies that fall within the first group, where the electronic ballot box, with or without a ballot, is the most commonly used device in all cases. The experiences of countries like Brazil [Re04] and India [In06] are noteworthy in this regard, particularly the latter, with its hundreds of millions of votes cast confirming the validity of this method.

In the second group, i.e. voting through telematic networks, which we have decided to call **telematic voting**, there have been few experiences with the status of official validity, although numerous proposals or voting schemes have emerged, defining the agents, procedures and security protocols necessary in order to carry out the voting process. In most of these schemes (of which [CC96] [OMA99] and [Ri99] are samples), determination of the security requirements to be met by voting systems has reproduced the guarantees provided by traditional voting processes, as these efforts have focused mainly on ensuring voter anonymity, preventing votes by voters that are either unauthorized or that have already voted and achieving an accurate vote tally. Moreover, since the voter is casting a vote through telematic networks, these voting schemes include cryptographic procedures that prevent votes from being altered or examined during their transmission to the ballot box.

1.1 Common solutions to basic problems

We shall now discuss in detail the problems faced by the designers of any system of telematic voting and the solutions most commonly adopted:

(1) Properly identify voters when casting votes; that is, there should be no usurpation of identity, for here no person can attest to voters' identity as is done at present in traditional voting with members of a polling station. The method for solving this problem is based, in every case, on the existence of a prior offline procedure involving distribution to voters of specific voting credentials that identify the bearer. These credentials today are found in many forms, from the simplest like a secret key to the most sophisticated, like a digital certificate.

(2) Guarantee the anonymity of voters, so that the credential used to validate a vote – and the voter's identity – cannot be associated with the vote cast itself. The most common solution to this problem is to divide the vote casting process into two phases: vote authentication and the voting process itself, so that distinct, unrelated entities will handle these two processes. Typically, the first entity verifies the credentials of the voter and grants permission to vote, while the second recognizes this permission and accepts the vote of the voter. Precautions must be taken to prevent any collusion between the two entities that might allow for establishing a relationship between the voter and the vote.

(3) Prevent voters from voting more than once. The solution to this problem is provided verifying the voter's credential, by simply marking a given credential as already used, with this status checked prior to giving permission to vote.

1.2 Threats posed by the use of computer networks and systems

In addition to the foregoing requirements to be fulfilled by any voting system, telematic voting systems must face specific threats: first, the fact of using communications networks to interconnect voting system devices, (voting sites, remote polling stations, etc) and second, the use of computer systems to cast votes or undertake counting procedures. Either of these conditions makes the following attacks possible:

(1) Attacks on the confidentiality of information and its integrity, making it feasible for an attacker to modify or eliminate votes legitimately cast or to discern their content.

(2) To counteract such attacks on telematic networks, the most advanced voting systems use cryptographic procedures that usually involve the application of ciphering algorithms of public keys and blind signatures to ensure the confidentiality and integrity of data, as well as to provide proof of the effective source of the same.

(3) These threats are compounded by the real possibility that the communications infrastructure could undergo a denial of service attack on voting day and thereby deny voters their legitimate right to vote. This problem is quite difficult to solve if voting is cast from home over the Internet, owing to the open, universal character of the net. Therefore, the usual countermeasures against this threat are based on constraining the scope of exercise of voting rights: voting from only specific places with the use of private virtual networks.

1.3 Telematic voting and alteration of results

Another danger faced by any voting system, whether traditional or not, is the possible alteration of the voting results from within the system itself. That is, when the results published do not truly reflect the votes cast (i.e., an election is rigged). In traditional voting, this risk is offset by the physical existence on paper of votes cast and the use of supervisors that monitor both the voting and tallying processes. However, in telematic voting, this risk is often underestimated, in spite of the fact that studies of the problem [Me01] indicate that one of the factors preventing social acceptance of these systems is the perception by citizens that it is quite easy to modify electronically stored data.

One of the solutions proposed to deal with this problem involves issuance of a receipt that would allow voters to be sure that the vote has been cast as desired. However, the existence of a receipt showing the vote poses the risk of its use as an element of coercion or sale of votes. Thus, alternative solutions have been discussed [Ch04], which in our view are not fully satisfactory, as they offer only an acceptable probability that votes have been included correctly in the tally.

Nevertheless, few voting schemes address the problems inherent in voting through telematic networks that require powerful verification tools to ensure the accuracy of results against possible collusion between system agents, while adding control elements for monitoring the proper execution of the entire voting process.

1.4 Solution proposed

This article proposes a system of telematic voting (called VOTESCRIPT), that reinforces verification processes as a crucial element to achieve full acceptance of the system by voters. Its most noteworthy features are the following:

a) Voting from specific sites (polling stations, kiosks) to avert both denial of service attacks and coercion of voters.

b) Use of a Java Card to store voting software and data related to the voting process. Inclusion of a receipt stored on the card, which is properly protected to prevent its use for coercion or vote selling.

c) Involvement of vote monitors to supervise and attest to the proper functioning of the voting process. The proposed system arises from the experience of this research group in contributing to the development of a theoretical model used by the Spanish Royal Mint to create its own voting system, for which field tests of the prototype were conducted in Ávila (Spain) in 03/2003. Smart cards technology available at that moment did not allow the prototype to fulfil all the specifications included in the theoretical model. Currently, a complete prototype of VOTESCRIPT has been developed making use of Java Cards.

2 Architecture

The VOTESCRIPT system is based on the use of blind signature algorithms as proposed by Chaum [Ch83] and a smart Java Card that would store the voter keys, the vote delivery applet and the voting receipt, among other things. It relies on the voting designs proposed by Fujioka [FOO93] and Cranor [CC96], while substantially improving upon them, as explained below.

2.1 Agents and persons

The communication scenario of VOTESCRIPT involves a set of automatic systems as follows:

(1) Authentication Points (APs). Computers equipped with card readers – but without cryptographic capacities – in which the voter engages in the authentication process.

(2) Ballot Points (BPs). Like the APs, these are computers equipped with card readers, though without cryptographic abilities, in which voters cast votes. A voter can cast a vote in any of the existing BPs.

(3) An Administration System (AS) that could be considered official, which authenticates voters.

(4) Several Intervention Systems (ISs). These are appointed by each of the groupings of electors or the candidacies authorized to supervise voting, with the mission of supplementing the work of the Administration System.

(5) A Ballot Box (BB) that collects votes cast and returns voting receipts.

(6) A Tallier (T), which could be considered official, for tallying votes following the end of the vote reception period. The key is a secret shared between the Administration and the Intervention Systems, and is obtained at the end of the vote reception period.

(7) Several Tally Intervention Systems to supervise the task previously performed by the official Tallier.

(8) Verification Points (VPs) to enable voters to see that their vote has been included and properly accounted for.

(9) A Tally Board that will hold the results published for a short period of time. The key is a secret shared between the administrator and the intervention systems, and is obtained when the individual verification process is performed.

(10) Voters. Each voter has a smart voting card, a Java Card that contains not only cryptographic algorithms specially designed for VOTESCRIPT, but which also executes part of the voter software.

(11) The Election Authority (EA). Consists of a group of persons responsible for general oversight of the system and charged with addressing any complaints.

2.2 Description of protocol

During the voting period, citizens that wish to vote will go through the steps described below, which constitute the VOTESCRIPT protocol (Figure 1).

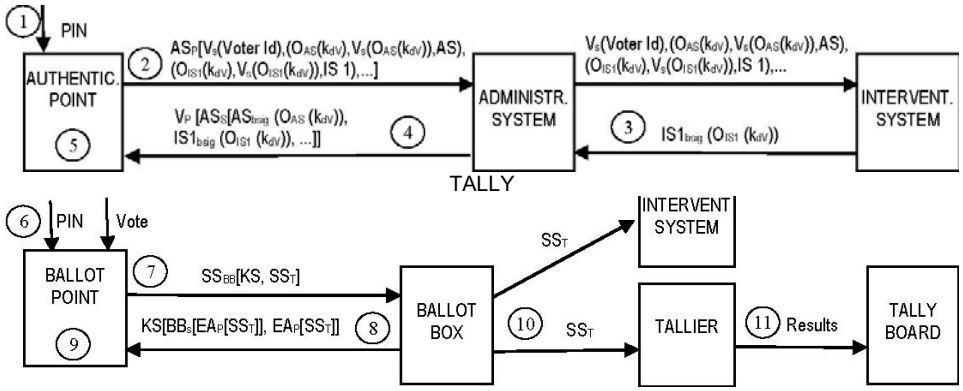

Figure 1: Voting protocol

Voter-Authentication Point Relationship

1 At the Authentication Point, the Voter inserts the Voter Card and is authenticated with a PIN or a biometric mechanism of identification.

2 The Voter Card, which contains two Voter keys – a public and private one – generates a pair of asymmetrical keys for voting (k_{dV}, k_{cV}) and a series of opacity factors. The key k_{dV} is opaque for the Administration System and for each of the Intervention System. The card signs the *voter ID* and all the opaque keys and ciphers the result with the public key of the Administration System. The Authentication Point sends this information to the Administration System.

AS_P [V_s (Voter Id), (O_{AS} (k_{dV}), V_s (O_{AS} (k_{dV})), AS), (O_{IS1} (k_{dV}), V_s (O_{IS1} (k_{dV})), IS 1), ...]

3 The Administration System reads and deciphers the data received and sends all the data to all the Intervention Systems. Each of the Intervention Systems, in the same way as the Administration System, checks that the Id is on the list of valid Ids, that the signature of the Voter making the request is correct and that the card has not undergone authentication previously. If not, the reception is rejected. If everything is in order, the Administration System and each Intervention System blindly signs the relevant opaque k_{dV} key.

4 The entirety of the opaque keys are signed by the Administration System with its private key and ciphered with the voter's public key, and then sent to the Authentication Point.

VP [ASS[ASbsig (OAS (kdV)), IS1bsig (OIS1 (kdV)), ...]]

5 The Authentication Point sends to the Voter Card the data received from the Administration System, so that the smart card receives the k_{dV} signed by the Administration System and by the Intervention Systems. It then verifies that the signatures are correct, and if they are, it stores them, so that they will constitute the vote delivery authorization for the voter during the voting process.

Voter - Ballot Point Relationship

6 At the Ballot Point, the Voter inserts the Card and is authenticated by means of a PIN or a biometric identification mechanism.

7 The Ballot Point asks the Voter to vote. In the Voter Card, the vote chosen is ciphered with k_{cV} and a piece of information is created with the ciphered vote, the k_{dV} and k_{dV} keys signed by the Administration System and the Intervention Systems. Then this piece of information is "stored" in a *T Secure Envelope* between the smart card and the Tallier. A *symmetrical* key (KS) is generated, joined to the T Secure Envelope and stored in a new *Secure Envelope BB*, which is sent to the Ballot Box.

SEBB[KS, SET]

8 The Ballot Box, after eliminating the *Secure Envelope BB* protecting the information received, obtains the *KS* and the *T Secure Envelope*. The Ballot Box stores the *T Secure Envelopes* received until the voting period is over. Based on the data protected with *T Secure Envelope*, it returns a receipt to the Ballot Point that preserves the anonymity of the voter. To generate the receipt, it performs the following operations: a) it ciphers *T Secure Envelope* with the public key of the Election Authority b) it signs it with its private key, and c) ciphers the receipt with the symmetrical key it received from the Ballot Point.

KS[BBs[EAP[SET]], EAP[SET]]

9 In the Voting Booth, information received is delivered to the Voter Card, which obtains the receipt, and it verifies the signature by the Ballot Box. The vote receipt is stored in the Voter Card and only the Electoral Authority can gain access to the data of the receipt in case of a complaint after the end of the voting process.

Opening the Ballot Box and tallying the votes

10 Opening the Ballot Box requires the physical presence of the Administrator and a sufficient number of scrutineers, who will insert their smart cards in the readers and authenticate themselves, either biometrically or with a PIN. The Ballot Box randomizes everything it receives and sends it to the Tallier and the Tally Intervention Systems, while also providing persons with management and supervision responsibilities over the electoral system a list of the data that has been sent. At that moment, all the information received by the Ballot Box during its operations is deleted. The restricted disclosure of the records transferred by the Ballot Box will help verify that the Tallier and the Tallier Intervention Systems are receiving the same information, so as to enable identification any element causing a malfunction in the event an alteration of the vote is detected.

11 The vote tally is then undertaken. Prior to reading the results, the System Administrator and the Scrutineers once again use their smart cards – with a shared secret procedure – to jointly provide the Tallier and the Tally Intervention System their private keys (which are stored and hided until that moment) needed to begin operations. After receiving all the information from the Ballot Box, the Tallier opens the T Secure Envelopes, performs the vote tally and sends to the Tally Board the information, composed of a kdV key and the kdV key signed by the Administration System and the Intervention Systems, along with the deciphered vote. The Tally Board announces the results of the vote to persons with management and supervisory responsibilities over the electoral system.

2.3 Voter Card

Along with the procedures designed to enable audits of software and the results, one of the pillars undergirding the strength of the proposed voting system is the possession of a smart card on the part of each voter. To meet the essential requirements of a voting system the smart card includes self-protection mechanisms against any attempt at reading or writing by equipment that is not standardized for the voting system.

The fact that all citizens make use of a smart card that enables them to sign information to offer proof of origin and decipher confidential information is not sufficient to provide the guarantees required by a voting system. A smart card is needed with cryptographic capacities that have been specially designed for this project, enabling performance of sensitive cryptographic processes, in addition to the usual tasks of identifying its holder. If performed outside the card, these processes would leave a trail of operations in machines that could be subject to subsequent analyses, with the intention of breaking the basic principle of secret voting.

The voter's smart card will internally generate keys for subsequent use. Among these are two pairs of asymmetrical keys: i) one composed of a secret key used to sign or decipher, and another of the public key, which is duly certified and disclosed by the responsible authority, to guarantee the identity of the holder. ii) The other pair is similarly useful to the prior one, but guaranteeing, this time, the anonymity of the holder. Cryptographic mechanisms ensure that the card bearer is a legitimate voter, that two voters will not have the same pair of keys, or that a single voter will not have more than a pair of keys for this use. The cryptographic procedures used will also ensure that no internal or external agent or collusion between them will be capable of disclosing the identity of the voter. This key will be used to legitimate the vote, which will come ciphered from the card so that it can be deciphered only by the Tallier in the tally phase.

Cryptographic processes to be executed inside the card also require the existence of a session key and opacity factors, knowledge of which by third parties would compromise the security of the system to the same extent as if the secret keys were disclosed. Thus, the smart card is the valid secure format, for it will generate keys and factors and, when necessary, share the keys with other agents; it will come from the card with all the confidentiality guarantees offered by cryptographic mechanisms, namely ciphering with the public key of the receiver.

Ciphering with a public key generally offers confidentiality guarantees; however, in voting processes, the number of messages to be ciphered is limited and sheer force may be sufficient to disclose the message. Thus, the card also includes the mechanism of random chains, which must also be generated inside the card, since it is indispensable that the chain be unknown to prevent successful violation of the secret vote.

For the purposes of use following publication of the results, the Ballot Box will give the voter a receipt for the vote. This receipt is designed so as not to expose the voter to the risks of coercion, since it is ciphered with the public key of the Electoral Authority. In this project, the citizen's smart card will securely store the receipt, having first verified its authenticity and storing it in a form that it can be read only by the Electoral Authority.

3 Individual verification and global verification

This project envisages two types of verification of results, which as a whole will act as a deterrent to temptations to commit fraud by the persons responsible for the operations of the different systems, since not only will the malfunction be detected, but also the system in which the malfunction has occurred will be identified unequivocally.

There are two types of verification: global and individual. Global verification of results is undertaken by candidates' representatives or by groupings of electors authorized to perform monitoring of the process. Individual verification is effected by the voter him or herself, with protection against possible coercion by means of properly designed procedures. As already described, the work of the Administrator during the voting process is supervised by the Intervention Systems in such a way that any anomalous issuance or denial of authorizations would be detected.

After the period provided for voters to deliver their votes to the Tallier, the content of the Tallier will be delivered to the Ballot Box and a copy of the data will be received in the Tally Intervention Systems, thus dissuading the Tallier from the intention of eliminating, adding or modifying votes. It would still be possible for the Ballot Box to destroy votes prior to delivering them to the Tallier and the Tally Intervention Systems. This circumstance – apart from raising less interest, since the destruction would be carried out against ciphered pieces of information, the true meaning of which is unknown – would be detected with individual verification procedures by means of the vote receipt signed by the Tallier and stored in the voter's smart card.

3.1 Global verification

Each Scrutineer will have a machine – Tally Intervention System – which will load a copy of the information that the Ballot Box delivers to the Tallier. This machine shall be audited in advance by experts trusted by system managers to achieve complete confidence that it can only perform a vote tally. Any divergence between the votes obtained by the Tally Intervention System and those obtained by the Tallier and published in the Tally Board would be a sign of an anomaly. Thus, neither the Tallier nor the Tally Board can alter – i.e., add, eliminate or modify – votes, nor will they are able to accept the validity of votes that have not been properly authorized. Both for lists of records received by the Tallier and for lists of information delivered to each candidacy, a validity period shall be in effect, so that once the specified time has elapsed and the election is considered valid, the lists must be destroyed in an audited procedure.

3.2 Individual verification

Once voting has concluded and the results have been published, each Voter can independently check that his or her vote has been properly accounted for. This verification is performed by a voter at their own initiative, with resources available to ensure their anonymity and protection from coercion. The Voter need only go to a Verification Point – in an individual manner – use the Voter Card and ask to be shown the vote associated to the information published by the Tallier and the information stored on the card. At this site, the same measures must be taken to ensure that the voter is protected against external surveillance as were taken when casting a vote at the Ballot Point. If the voter does not accept the vote shown at the Ballot Point, the person may appeal to the collegial body called the Electoral Authority, which is responsible for overseeing the proper functioning of the system, and which addresses all complaints lodged by voters. When a complaint is made by a voter regarding treatment of their vote, the Electoral Authority can obtain the vote receipt stored in the smart card of the voter and will use all cryptographic proofs available in the system to investigate the validity of the complaint. The Electoral Authority will obtain solid cryptographic proofs to determine where the anomaly lies and what agent is responsible for it.

4 Innovations of VOTESCRIPT system

This section highlights the main innovations provided by the VOTESCRIPT system, with a comparison of the solutions it proposes with those contained in the main voting schemes used as a reference in this field.

(1) The VOTESCRIPT system provides an individual verification system that enables each voter to check, in specific places and during a determinate period of time, whether their vote has been properly included and accounted for. The innovation as regards other solutions lies in the fact that the process is private, as the voter can at no time show to unauthorized third parties the content of the vote, thus preventing the buying and selling of votes or extortion.

(2) The existence of Intervention System is one of the main innovations of this system, since it enables monitoring of the entire electoral process by groupings of citizens or by duly authorized candidacies. Global verification made available to scrutineers provides solid cryptographic proofs that make it possible to demonstrate unequivocally whether the system has operated fraudulently or not.

(3) The cryptographic cards designed for the project guarantee the identity of the voter, and also perform all functions of ciphering and deciphering, generate of session keys and authentication of signatures in the card itself, with the aim of blocking access to critical information by malicious users. The voter card is a Java Card that contains vote-casting software, while it stores certain information associated to the vote¬casting process, the receipt, with a view to enabling subsequent verification.

(4) There is a collegial body called the Electoral Authority, which is charged with the tasks of overseeing the proper functioning of the system and addressing any complaints made by voters. In the event of a complaint by a voter about the treatment given their vote, the Electoral Authority shall discover and compare all the cryptographic proofs in the system in order to check the validity of the tally.

(5) The system also ensures that the content of a vote cannot be disclosed in the future. Cryptographic presentation of the vote through cryptographic algorithms means that these systems cannot gain knowledge of the vote's content, but it does not ensure that the advancement of cryptoanalysis will not enable it to be known in the future.

5 Conclusions

Today, experiences in telematic voting abound, and these initiatives always highlight the benefit for voters of being able to cast a vote from any computer connected to the Internet. However, the euphoria seen in these experiments makes both organizers and voters overlook the fact that these systems are unable to demonstrate that the results published have not been tampered with prior to their release.

The system presented herein is fully verifiable, as the system's strength lies in its provision of cryptographically solid and secure pieces of information that can be used as proof before third parties in case of litigation or rejection of the results of the process. In the VOTESCRIPT system, as in other recent proposals for telematic voting, the smart card serves as a security token that allows for the protected storing of private keys that enable the voter to undertake authentication in the system and cast a vote in reliable manner. Nevertheless, the smart card plays a much more important role in VOTESCRIPT than these other systems.

The system presented constitutes a valid solution to traditional problems of voting systems, and it can counteract the understandable wariness of voters towards telematic voting processes. E-voting systems that aspire to replace traditional voting systems must include the positive aspects of these traditional arrangements, while offering new functionalities such as those presented here in order to deserve the trust of the citizenry.

References

[CC96] Cranor, Lorrie F.; Cytron, Ronald K.:. Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA, 1996.

[CGP02] Carracedo, J.; Gómez, A.; Moreno, J.; Pérez, E.; Carracedo, J.D.: Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT). II Congreso Iberoamericano de Telemática. CITA'2002. Mérida, Venezuela. 2002.

[Ch04] Chaum, D.: Secret-Ballot Receipts and Transparent Integrity. IEEE Security & Privacy. Vol 2 N1. January-February 2004; pp 38-47.

[Ch83] Chaum, D.: Blind signatures for untraceable payments. Advances in Cryptology, Crypto '82, Springer-Verlag, Berlin. 1983; pp. 199-203.

[In06] Indian Voting. http://www.ensl.cs.gwu.edu/voting/India, last accessed February 2006.

[Me01] Mercuri, R.: Testimony presented to the U.S. House of Representatives Committee on Science. http://www.house.gov/science/full/may22/mercuri.htm. 2001.

[OMA99] Ohkubo, M; Miura, F.: Abe, M.; Fujioka, A.; Okamoto, T.: An Improvement on a Practical Secret Voting Scheme. Lecture Notes in Computer Science 1729, Springer-Verlag, Berlin, 1999; pp. 225-234.

[Re04] Rezende P.: Electronic Voting Systems. Is Brazil ahead of its time?. Cryptobytes, Vol 7, N. 2, RSA Security Laboratories, USA. Fall 2004; pp. 2-8. http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_Fall2004.pdf, last accessed February 2006.

[Ri99] Riera i Jorba, A.: Design of Implementable Solutions for Large Scale Implementable Voting Schemes. PhD thesis, Universitat Antónoma de Barcelona, 1999.

A preliminary question: Is e-voting actually useful for our democratic institutions? What do we need it for?

Jordi Barrat Esteve

Dept. Dret Públic (SEJ2004-03844JURI / LEO26A05)
Universitat Rovira i Virgili
Avda. Catalunya, 35
43002, Tarragona, Catalonia / Spain
jordi.barrat@urv.net

Abstract: The current development of e-voting systems worldwide raises several specific interesting issues from a legal point of view. Auditability measures, identification procedures or guarantees for voting secrecy and equality are good examples, but we often forget a fundamental question: the usefulness of these new technologies. This paper intends to provide an answer that takes into account the complexity of all democratic systems. An updated image of the electoral procedures, the advantages for disabled people, the reduction of economic charges in the electoral fields or the increase of voting turnout will be analysed as the possible positive consequences of e-voting systems.

1 Presentation

The theoretical arguments about e-voting procedures often begin with a couple of general statements that it is worth recalling. First of all, political participation cannot – and should not— remain isolated from the vertiginous development of ICT. In the future, these new technologies will condition, with even greater intensity than nowadays, the ways popular will is expressed and, probably, votes are cast.

On the other hand, fears are also voiced about the dangers of a non-reasonable transformation of political participation channels. New values could appear and the supreme democratic goals could suddenly be found to be secondary to the use of new technological tools. Basic principles, such as equality and freedom, the secrecy of the vote, the consolidation of free public opinion or the existence of enough socialization areas should then not be displaced by other narrow strategies favouring the use of ICT.

It is very difficult to disagree with these obvious statements, but there are others, both positive and negative for e-voting systems, which are too generic. They are very short on analysis and do not take into account the complexity of these technical developments. This paper intends to provide some specific theoretical elements about the role of e-voting procedures in our democratic institutions [for a general overview, see Tu05, Gr03, KB04, PK04 and TM05].

It will not therefore consider such important specific issues as auditability measures for e-voting systems or identification procedures in remote voting. We will remain at a preliminary stage and discuss whether e-voting is actually useful for us.

2 Necessity and usefulness of electronic voting systems

Electoral institutions already accept computer procedures in some processes like the roll out or the transmission of results, but we should try to determine whether these technologies could also be useful tools for casting a vote. The physical identification of a voter, a transparent urn or an isolated booth are main elements in our electoral scheme and we would like to know if they need technical updating, maybe with e-voting solutions, or whether the current structure is better. The answer should not depend only on technological optimism because tools can easily become a goal in themselves and this situation could not be considered as an advantage for the electoral system. The only way to accept these innovations is to prove that they will be useful for citizen participation and, in a more specific way, for the vote casting.

The specific answer will depend on the electoral systems and a variety of parameters should be taken into account. For instance, many political institutions have no important problems and there is no legal or social necessity to make changes. Most European countries follow this model. Electoral discussions focus on the eligibility formula (proportional rules, etc.), but they do not foresee the need to modify electoral procedures that have been tested in several elections and accepted by everybody (I). In these cases, is it actually a priority to introduce e-voting mechanisms? Would they maybe generate inherent dangers that could weaken a popularly accepted system such as the current one?

In our understanding, these are correct and reasonable concerns given that we are dealing with highly sensitive areas in which the expression of the sovereign will is at stake. It would not, therefore, be wise to introduce innovations whose consequences have not been sufficiently analysed and compared. Even so, we believe that there are several reasons for encouraging a slow introduction of electronic voting systems.

It should be noted, in the first instance, that electoral procedures should not be limited to an *outdated technological framework* because it would give our current modern society a poor image. As Michael REMMERT points out «modernising how people vote will not, *per se*, improve democratic participation but failure to do so is likely to weaken the credibility and legitimacy of democratic institutions» [Re03: slide 34]. This initiative, however, cannot ignore the correct functioning of many electoral systems. If REMMERT's statement is understood to be saying that we have no choice to make in electoral modification, that there is an unavoidable necessity to change the current systems by introducing new technologies, it will not be acceptable. I think, however, that REMMERT's quotation can help us if we reduce its sense. Obviously, we should not forget the reasonable results of current elections, but we should always search for innovations that not only maintain the traditional electoral guarantees of any democratic system but also provide other advantages. As REMMERT foresees, our not doing this will probably decrease the system's legitimacy because, although the organization is correct nowadays, efforts must be made to keep the system up to date. Constant awareness must be maintained so that, without endangering the success and stability already reached, electoral processes gradually incorporate the technologies that characterize our era.

On the other hand, the electronic vote can be enormously *useful for certain sectors of society* (for example disabled citizens, absent residents). These are groups that often encounter many problems when it comes to exercising their right to vote, and new technologies, if designed correctly, could facilitate their participation considerably. It would therefore be possible, for both groups, to vote remotely and, in the case of the blind, electronic tools could even allow an autonomous polling-station vote.

The current low turnout of residents living abroad has several explanations, but two of them are, without doubt, the bureaucratic effort they have to make in some cases and the important role of the postal administration of different countries with very narrow deadlines [see Ca03]. Voting from abroad therefore is not simple, but Internet voting could maybe make it much easier.

Disabled citizens could always use these new voting channels. Electronic devices would make it possible for blind people to cast their votes autonomously. Spanish legislation (art. 87LOREG) currently provides disabled voters with the possibility of an assisted vote, but, even though this is a reasonable solution, it is certainly true that e-voting would allow even blind people to make a vote without help and this is obviously a great advantage.

These considerations show that it is important to define the typology of e-voting systems because not all electronic procedures will provide good solutions for disabled people. While the computer- and even mobile-phone applications more easily accept specific devices for disabled people, other e-voting systems, like those based on optical ballots, are considerably less useful from this point of view.

Blind people, for instance, will not be able to use optical ballots because they cannot have audio devices. Printing *braille* ballots could be a solution, though costly, but it is not e-voting. What is more, the separation of paper ballots into Braille and non-Braille could become a serious problem for the secrecy of the vote (see Resolution *Junta Electoral Central* / January 31st 2000; Fu00: 43-44).

In conclusion, the analysis of the usefulness of e-voting procedures should take into account the differences among them because they all have different frameworks.

Thirdly, electronic voting systems are more *versatile and flexible* than anything previously known. Today, the logistics surrounding elections involves economic, time and human costs that make it difficult for them to be conducted frequently. Some electronic voting models –not all– simplify this process and make it possible to imagine a future in which more participation tools could be made available to citizens. It should also be mentioned, not forgetting the important factors regarding security, that a good electronic voting system would be much more exact and precise than the current one. As Andreu RIERA, the person in charge of Scytl pointed out during the presentation of the citizen consultation *MadridParticipa*, there are still «muchos más errores en papel que en formato electrónico» ("many more errors on paper than in electronic format").

However, are these new participation channels actually good? Should we back an electoral system that includes the remote vote from home? Would it be a democratic advantage or a disadvantage? These questions are closely related to the theoretical analysis of democratic representation, which is now experiencing difficult moments. Increasing direct citizen participation could be one solution because it is an attempt to reduce the role of the political parties by empowering citizens with new participation tools.

However, even people who agree with this proposal often stress the dangers of a massive introduction of direct participation tools. Democracy is both casting a vote and having a society with a sensible way of life. It needs to provide citizens with information and create debate among them so that political ideas are to mature sufficiently. To recklessly promote an increasing number of consultations could have negative collateral consequences for the democratic system. And, if this is so, is the convenience of e-voting tools, and the resulting almost effortless multiplication of our voting potential, actually an advantage? Should we consider it to be positive?

Despite all the above, a well-designed democracy based on citizen participation is always a good initiative and, in the future, there will probably be more opportunities within this framework to accept direct and binding citizen consultations. E-voting solutions can facilitate this path as long as they reduce the economic and logistic cost of an election, but this does not automatically mean that they must be massively implemented. There will be the option to do so, but those responsible for the democratic process should evaluate whether it is advisable.

Whatever solution we adopt, there is another issue that is closely related to this one. Many authors think that Internet voting may endanger the public nature of the voting day because the changes in the *electoral routine*, an essential component for any democratic procedure, allow votes to be cast from private places (companies, home, etc.). The political socialization process, then, will be different and it could also generate different and maybe negative political values because there will not be a physical relationship among voters. Following the explanation of Andreas AUER and Alexander TRECHSEL, «le citoyen n'irait plus voter en pensant à l'intérêt général, mais il voterait en tenant compte uniquement de son propre intérêt» [the citizen will not vote considering the general interest, he/she will only consider his/her own interest] (AT01: 45-46; see Su01).

I think however that this strong defence of the current electoral routine is a direct consequence of the system's weaknesses and it should strengthen the need for a democracy with more participation channels. If a short one-day meeting has become an essential component in our democratic behaviour, it is clear that we have a serious problem because the political system is not actually progressing. The relationship between citizens and their representatives cannot be reduced to an occasional point of contact and political socialization should not rely upon this small parameter. It should be a day-to-day process. Within this normal democratic framework, the absence of one act of socialization as a consequence of the introduction of Internet voting should be of no importance and it should be easily accepted.

It should also be noted that there could be virtual socialization areas. New technologies have such interactivity and simultaneity that they can emulate physical meetings and thus create complementary socialization channels. The above-mentioned authors use the following argument to respond to criticism: «il est plus probable que dans le contexte social actuel, une prise de conscience plus compléte des enjeux sociaux d'une votation se fasse à travers les informations et les débats que les citoyens pourront avoir sur Internet avant de voter» [in our current social framework, the use before voting of Internet information and on-line debates will probably generate a more complete idea of the social challenges of an election] (AT01: 46; see KK05).

Anyway, some e-voting procedures do not change the current electoral liturgy. Optical ballots, for instance, are usually presented as mechanisms that do not alter voting behaviour and this is their main advantage. Moreover, both computers and telephone devices can be used in official polling stations, so they will not change the current socialization process during the voting day.

However, the economic advantage of e-voting seems to be linked with the use of non official places for casting a vote because, if we maintain the current network of polling stations, there will be no decrease in logistical obstacles or economic expenses. The possibility of asking citizens for their opinion more frequently also disappears. Optical ballots need the same number of polling stations and they will be more expensive because, even if the current combination of paper and urns is maintained, the ballots contain electronic devices that will probably increase their price.

However, the other e-voting systems, with computers and phones, are not necessarily cheaper. If they are used within official polling stations, our conclusions here are the same as those of the paragraph above. If they are used from other places, the logistical organization could be less, but the final cost will depend on the development of the computer applications and security measures that they need. Both of these situations may be cheaper or more expensive than the current paper ballot system. This depends on the fees determined by the computer experts.

Finally we should note that *election turnout* could increase as a result of implementing electronic procedures. It is frequently mentioned that the use of new technologies would make voting more attractive and certain segments of the population that traditionally abstain, such as young people, may change their attitude with these measures. The fact is, however, that there are no conclusive studies. While some experiences show that the electronic vote increases participation, others indicate the opposite. As a guide, we should mention the tests undertaken during the last Catalan elections in which certain absent residents, among whom were the Catalans living in Mexico, were allowed to use the Internet experimentally to vote. The number of participants exceeded the number of official voters by 226% (see BR04: § 3 / table 3). On the other hand, other experiences show very low rates. For example, in the MadridParticipa citizen Consultation in 2004, only 0.63% of the total electorate took part (see BR04a). The absence of precedents, however, makes it difficult to compare and to conclude whether new technologies encourage more or less participation. There are a number of variables that influence these results (e. g. a consultation is not the same as an election). Nor is it the same if electronic systems act in a unique or complimentary way. Lastly the method used also influences the process: systems based on remote voting in non-controlled environments do not present the same degree of difficulty as models based on optical paper-ballots.

The number of voters is only one parameter, but there are others that also have an important influence on increasing the quality of a democratic system: the *geographic distribution* of votes and the way votes are cast.

The Barcelona Technical Engineering Association (CETIB) is a good example of the first one. Before June 2005 the members of this Association could renew the presidential board every four years by voting through only one channel. There was an official polling station in the Association's main building, in downtown Barcelona, but this electoral organization was disadvantageous for those members who did not live there. For instance, if we analyse the previous results, it is easy to prove that the percentage of Barcelona inhabitants who voted was higher than the percentage of citizens of this city on the census. Neither did total turnout rates ever reach 10% of the electoral roll.

Therefore, in June 2005, the Association's Board decided to accept two voting channels. They intended to increase the total number of voters and also to balance the privileges of some members with a new distribution of votes from a geographical point of view. Each electoral county was to have the same proportion of voters and registered members.

Unfortunately, the turnout decreased in June 2005, but there was significant progress in geographical balancing. As Oriol CISTERÓ'S graphs indicate, the *Barcelonès* County, including the capital Barcelona, decreased from 71 to 64 per cent of the votes cast while its proportion of members was 50% (2005: slide 14).

The second graph, which refers to the e-voting channel is even more significant: if we analyse the geographical distribution of votes, the new balance more accurately reflects the percentage of members. In this case, the *Barcelonès* County represents only 53% of the votes, which is very close to the 50% of registered members living in this electoral district (Ci05: slide 15).

Beside the total turnout and the geographical balancing, another parameter was used to evaluate the success of the e-voting procedures: *the way votes were cast*. The acceptance of electronic means in the General Assemblies of Spanish companies with stockholders is a good example.

The initial situation is very negative because these Assemblies often have a considerable democratic deficit. Most stockholders do not go to the meeting and they delegate their votes. The company admistrators themselves encourage these delegations. Therefore, the company has an internal democratic functioning, but only from a formal point of view. Massive delegations also make the control task that belongs equally to all stockholders more difficult.

In view of this situation and as a result of new corporate governance rules, the Spanish Act 26/2003, about transparency in stockmarkets, added two new paragraphs to article 15 of the Spanish legislation on the companies involved. The first one provides for a vote in the General Assembly cast by electronic means: «de conformidad con lo que se disponga en los estatutos ... podrá delegarse o ejercerse por el accionista mediante correspondencia postal, electrónica o cualquier otro medio de comunicación a distancia» ("in accordance with what is stipulated in the statutes…it may be delegated or executed by the shareholder by postal mail, electronic mail or any other means of remote communication"). This legislation is a direct consequence of the ALDAMA report, the main document produced by a specific Commission created to analyse the transparency and security of the financial markets. Among other issues related to Stockholders Assemblies, this text recommends that e-voting mechanisms be used: «implantar los sistemas necesarios para el cómputo electrónico del quórum, así como para la delegación y el voto por correo o por medios electrónicos» ("to implement the systems required to electronically compute the quorum, and to delegate and vote by mail or electronic means") (In03: 32). There are no other similar Acts in Spain, but VAÑÓ VAÑÓ thinks that this lack does not prevent these electoral procedures from also being included in other financial companies like those based on a collective property of the workers themselves –*credit unions / cooperativas de crédito*— (Va04: 136-137).

Several companies have already modified their internal rules and there have already been the first cases of stockholders voting remotely. The possible simultaneous casting of votes, remotely or traditionally, during the Assembly itself creates considerable technological challenges related to digital identification procedures.

There are also specific rules for delegating the right to vote (see Va05: 225-255). Some pioneer experiences, like Union Fenosa in 2003, had no positive results because only one stockholder finally cast his/her vote (see Va05: 24), but subsequent experiences were successful in consolidating a new democratic framework for these companies.

Shortly, even with the same turnout rates, e-voting procedures can offer other significant advantages like the option of a direct and personal vote. There would be no more voters, but the internal structure of these companies would have improved from a democratic point of view.

Anyway, we should not forget that abstentionism in our Western societies has deep roots and does not depend only on the ease of voting (see An99). Simplified voting procedures, like those provided by some e-voting systems, may eliminate some of the reasons for current abstentionism, but obviously not all of them.

Having analysed the arguments in favour of e-voting solutions in countries with consolidated democratic systems, we conclude that, even with trustworthy electoral procedures, new technologies could enrich citizen participation mechanisms.

In any case, not all countries have consolidated systems. Many states make enormous efforts to increase the reliability of their electoral logistics, but are often confronted with corruption, disinterest or with the illiteracy of large segments of the population (II). Can the electronic vote provide positive solutions to this worrying situation? Would we not perhaps be making a mistake by attempting to introduce sophisticated technological mechanisms in countries whose priorities, as we have seen, should be others?

The answer to this question depends not only on the situation with which we are confronted but also on the technological option chosen. Firstly, we should be aware that, although we may find that some countries have structural deficiencies in the socio-electoral area, the differences between them could be so considerable that it is not possible to have a generic approach to questions that require individual study. It should also be said, however, that even in extreme cases the electronic vote can provide positive new aspects.

Brazil and India can serve as a reference given that they are countries where the logistics surrounding elections present very serious problems. Their geographical dimension, corrupt attitudes and the widespread poverty and illiteracy are enormous challenges for any proposal that plans to develop a democratic process. Despite all this, both countries are using electronic ballots.

Brazil, for example, has been able to generalize the use of electronic voting by way of touch screens (see Ri03: § 31-47). The important aspect of this case is that technological modernization has helped to reduce some of the deficiencies mentioned above. In this way, the design of the screen, which emphasized such graphical elements as the photo of the candidate, has allowed both complete and functional illiterate people to exercise their right to vote in a simpler, more intuitive and safer way than the traditional ballot. On the other hand, the fact that computers automatically count all the votes could help to prevent, although not eradicate, the traditional dangers of electoral corruption.

In the case of India**,** elections in 2004 have demonstrated that it is possible to introduce extraordinarily simple electronic systems (see Te04; Id04). Although the model may contain some defects, the novelty of the experience was that it tested a range of electronic voting tools that were not complex but could modernize the Indian electoral process at a reasonable price.

3 Concluding remarks

Having analysed examples from both developing and developed countries, we can conclude that legal electoral regulations cannot be excluded from technological innovations such as electronic voting systems. There are several reasons for this: the need to prevent outdated political systems, the fact that the political participation of specific groups can be improved or the possibility that the current electoral corruption in some countries can be reduced. These innovations should naturally be undertaken with care**.** There is no room for adventurous behaviour, which disregards the virtues of the current systems and hopes to improve these with excessive naivety or technological optimism. It is not admissible, for example, that the electoral fiasco that took place in the United States in the 2000 presidential elections be hastily resolved by way of introducing electronic ballot boxes that had not been adequately controlled (see KSR04). The scandals that have arisen in relation to firms such as *Diebold* do very little in favour of a technological modernization process that, if appropriately implemented, is already an imperative need in current democratic systems.

Neither is it possible to accept those strategies that try to make massive e-voting evaluations without clear rules governing the attendance of independent observers or without officially publishing the results of the survey carried out during the electoral days. Unfortunately, the Spanish Government made these mistakes in 2005 during the referendum on the European Constitution.

4 References

[An99] Anduiza Perea, E.: ¿Individuos o sistemas? Las razones de la abstención en Europa occidental. Centro de Investigaciones Sociológicas, Madrid, 1999.

[AT01] Auer, A.; Trechsel, A. H.: Voter par Internet? Le projet e-voting dans le canton de Genève dans une perspective socio-politique et juridique. Helbing & Lichtenhahn, Bale, 2001. *www.geneve.ch/evoting/doc/voter_par_internet.pdf* [November 30th 2004]

[BR04] Barrat i Esteve, J.; Reniu i Vilamala, J. M.: Informe de las experiencias de voto electrónico empleadas en las elecciones catalanas de noviembre 2003. Universidad de León – OVE / Universitat de Barcelona, León / Barcelona, 2004. *www3.unileon.es/dp/aco/area/jordi/treballs/evot/cat03.pdf* [November 30th 2004]

[BR04a] Barrat i Esteve, J.; Reniu i Vilamala, J. M.: Democracia electrónica y participación ciudadana. Informe sociológico y jurídico de la Consulta ciudadana "MadridParticipa". Ayuntamiento de Madrid, Madrid, 2004. *www3.unileon.es/dp/aco/area/jordi/treballs/evot/llibreesp.pdf* [November 30th 2004]

[Ca03] Calderón Chelius, L. (coord.): Votar en la distancia. La extensión de los derechos políticos a migrantes, experiencias comparadas. (Col. "Contemporánea Sociología"), Instituto Mora, Mexico DF, 2003.

[Ci05] Cisteró i Fortuny, O.: E-Vot vinculant per Internet. Eleccions als càrrecs de la Junta de Govern del Col·legi d'Enginyers Tècnics Industrials de Barcelona. Juny 2005. In: II Jornades de Signatura Electrònica. Agència Catalana de Certificació – CATCert, Barca, 2005. *www.js-e.net/cat/Archivos/ponencies_web/Oriol_Cistero.pdf* [January 5th 2006]

[Fu00] Fundació Jaume Bofill: La votació electrònica: un debat necessari. (Col. "Debats de l'Aula Provença – 33"), Fundació Jaume Bofill, Barcelona, 2000.

[Gr03] Gritzalis, D. A. (ed.): Secure Electronic Voting. Advances in Information Security. Kluwer, Boston, 2003.

[Id04] IDA – Interchange of Data between Administrations: India's massive e-vote considered a success. IDA / European Union – eGovernment News / May 17th 2004. *europa.eu.int/ISPO/ida/jsps/index.jsp?fuseAction=showDocument&documentID=2551&parent=chapter&preChapterID=0-140-194* [May 21st 2004]

[In03] Informe: Informe de la Comisión especial para el fomento de la transparencia y seguridad en los mercados y en las sociedades cotizadas. Comisión especial para el fomento de la transparencia y la seguridad en los mercados financieros y en las sociedades cotizadas, 8th January 2003. *www.cnmv.es/publicaciones/informefinal.pdf* [November 30th 2004]

[KB04] Kersting, N.; Baldershein, H. (eds.): Electronic Voting and Democracy: a Comparative Analysis. Palgrave Macmillan, Basingtoke, 2004.

[KK05] Kies, R.; Kriesi, H.: Designing internet voting. The potential impact of a pre-voting public sphere on pre-electoral opinion formation. In (Trechsel, A. H.; Mendez, F., Eds.): The European Union and E-voting. Addressing the European Parliament's internet voting challenge. Routledge, London, 2005; pp. 147-165.

[KSR04] Kohno, T.; Stubblefield, A.; Rubin, A. D.; Wallach, D. S.: Analysis of an Electronic Voting System. 2004 IEEE Symposium on Security and Privacy, 2004. *avirubin.com/vote.pdf* [August 18th 2004]

[PK04] Prosser, A.; Krimmer, R.: Electronic Voting in Europe. Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, 2004.

[Re03] Remmert, M.: Developing a common framework for e-voting in Europe: The Council of Europe's draft recommendation on the legal, operational and technical aspects of e-voting. ACEEEO – Association of Central and Eastern European Election Officials, Annual Conference / London – October 2003. *www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2Dvoting/04%5FBackground%5Fdocuments/07_Presentation_MR.asp#TopOfPage* [August 17th 2004]

[Ri03] Rial, J.: Modernización del proceso electoral: voto electrónico. Observatorio Electoral Latinoamericano, [2003]. *observatorioelectoral.org/biblioteca/?bookID=26* [August 18th 2004]

[Su01] Sunstein, C. R.: Republic.com. Pricenton University Press, Princeton.

[Te04] Techaos: Indian EVM compared with Diebold. Tech Caos, personal blog / May 13rd 2004. *techaos.blogspot.com/2004/05/indian-evm-compared-with-diebold.html* [July 28th 2004]

[TM05] Trechsel, A. H.; Mendez, F. (eds.): The European Union and E-voting. Addresing the European Parliament's internet voting challenge. Routledge, London, 2005.

[Tu05] Tula, M. I. (coord.): Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales. Ariel, Buenos Aires, 2005.

[Va04] Vañó Vañó, M. J.: Transparencia y nuevas tecnologías en las cooperativas de crédito. In: CIRIEC-España, Revista economía pública, social y cooperativa. 49, 2004; p.117-141.

[Va05] Vañó Vañó, M. J.: Derecho de sociedades y comunicaciones electrónicas. In (Plaza Penadé, J., Coord.): Cuestiones actuales de derecho y tecnologías de la información y la comunicación (TICS). Aranzadi, Cizur Menor, 2005; pp. 225-255.

How e-voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals.

Laurence Monnoyer-Smith

Dept. of Human Sciences and Technology
Université de Technologie de Compiègne
BP60319
60203 Compiègne Cedex, France
laurence.monnoyer-smith@wanadoo.fr

Abstract: This paper describes the direct relationship between the perception of citizenship and its material expression, with emphasis on how changing expression obliges a rethink of the channels of mediation between citizens and their elected leaders. An analysis of the French voting ritual will show how our voting system is embedded in a specific cultural conception of citizenship . The emergence of new voting procedures could then be analysed on a social point of view as the will for citizens to rejuvenate some ancient conception of citizenship. I propose a table which maps out the connection between citizenship models and their new technological materialization. A two-way flow of creativity between models and tools which broadens scope for grassroots participation then explains the creation of new rituals as well as the reframing of the role of existing rituals.

1 Introduction

Electronic voting has been gradually establishing itself in the political landscape as voting terminals and online voting replace the traditional ballot boxes of Europe and punchcard machines of the U.S.A [Co02], [KLS04], [No04], [TM05]. Beyond the design issues, voting technology demands new legislation that requires re-examination of the fundamental principles of citizenship and representation developed and applied since the birth of our modern democracies some two centuries ago. While the debate on data security issues and costs has been running since the beginning , the fundamental question of how to adjust existing theoretical models of citizenship to cope with new forms of online democracy has been assessed more recently [CM01], [Ho01], [Sa01], [Co01], [Co05a,b], [Mo03]. As such, the virtual ballot introduces disturbing modifications to the material procedures of the voting ritual [MM02], [OV04], [KLS04]

This paper describes the direct relationship between the perception of citizenship and its material expression, with emphasis on how changing expression forces a rethink of the channels of mediation between citizens and their elected leaders. The availability of new mediation channels need not be seen as the disappearance of a time-honored ritual but as a symptom of change in how voters experience their citizenship. This allows reinstatement of procedures according to a pre-selected model of citizenship that follows

the trend and clearly identifies the risks before technology-based decisions impose restrictions with no public debate. For the purpose of this paper and as an example, I have chosen to describe how new voting technologies challenges the French ritual voting procedure.

2 The Rise of Online Voting

Dreams of better voting systems date back to the early 20th century, largely inspired by rising numbers of voters, multiple elections falling the same day and second-round run-offs that caused many countries to consider replacing ballot boxes with "voting machines"[No04], [Ih93]. However, mechanization was limited to putting some buttons and vote counters in a booth before interest waned fatally after the unpromising results of 1970s trials in Europe and North America.

Only in the late 1980s did the first electronic systems come online, entering use on a national scale in Belgium and Holland in the early 1990s and Brazil in 1996. For its part, France ran a few trials in Bordeaux and Brest in 1980 but the real test of the all-in-one electronic booth with a "built-in ballot box" was the 1999 European Union elections, followed by its use for the 2000 referendum asking citizens whether or not to reduce the presidential term of office from seven to five years. The success of these two experiences led the Interior Ministry to approve three different types of electronic voting systems in its Decree of 18 March 2004.[1] All three are compatible with the traditional voting station but eliminate the need for a ballot box. Without directly threatening the physical survival of traditional voting devices, the systems nonetheless mark a step towards fundamental subversion of the traditional voting process itself[2].

Meanwhile, the Internet started fostering the first political and administrative applications of either technocratic or community-based inspiration in North America and Europe [Ts00]. Most of the first private-sector initiatives were from the U.S.A. where a handful of manufacturers, with a background in onsite/online voting and secure online transaction systems, began to market online voting systems for general meetings of corporate shareholders and of professional associations. In Europe, Germany, Switzerland and the U.K. began studying new voting technologies in the mid-1990s through a series of pilot projects involving television, SMS, postal votes, etc [Mo03]. However, the European Commission (E.C.) soon took the lead in online voting through its Fifth Framework Programme for the User-friendly Information Society [Mo04][3]. By the mid-1990s, the E.C. was a very proactive backer of "digital city" projects, online voting and electronic services, thereby giving Europe a decisive lead in hands-on experience over the U.S.A. where initiatives were more limited.

The issue of remote, online voting differs radically from that of straightforward electronic voting in a polling station because it directly undermines the material basis of

[1] The NEDAP 2.07, RDI-Consortium Univote iVotronic and the Indra Sistemas SA Point & Vote
[2] - For an exhaustive analysis of French experiments in electronic voting systems, see Ledun, 2005.
[3] http://europa.eu.int/comm/research/ist/leaflets/en/whatisthe5th.html.

the electoral process, something the 1975 French ban on voting by mail sought to protect. Thus, one major consequence of online voting is the denaturing of a voting process, even if it has existed in its present form for less than a century [Ih93]. At this point, two attitudes strike me as mistaken. The first is to perceive the new technologies as a threat to a time-honored voting ritual – an opinion widely held among elected officials and researchers in France. The second is to reduce the technologies to a process of mass rationalization of government administration that transforms the citizen into a consumer, thus assimilating the political and economic systems into Niklas Luhman's autopoietic concept of society [Le05]. They are mistaken, I find, because both disregard the social substance of the technological devices. Indeed, voting should be analyzed with all the methodological rigor due to any "total social phenomenon", to quote Marcel Mauss. A full discussion is beyond the scope of this paper but I shall stress the complex interplay of all the dimensions proper to voting (e.g. political, social, economic, technological, legal, communicational) and the need for taking perspective in an area where, more so than elsewhere, the observer is part of the thing observed.

For these reasons, it is pointless to deny that electronic voting undermines a fundamental symbolic construct of our contemporary democracies or that online voting was developed by private enterprise in a bid for a share of e-government markets [KLS04], [OV04]. That said, in light of the above considerations, it is important to note that the introduction of online and other new voting technologies is a symbolically and politically loaded event of a magnitude equal to the introduction of the now-familiar ballot box some 150 years ago.[4] To ignore this is doubtless to misinterpret the call of a part of society that is becoming manifest after the emergence and local appropriation of these new technologies and, doubtless, to remain prisoner of one's own mindset.

3 The Paper Ballot as a Ritualization of Citizenship

The protocol of the voting ritual is a system of constraints, a set of procedures and a symbolic construct that incarnate a set of beliefs. The more this symbolic dimension is anchored in a country political culture, the harder it is to investigate on new voting systems. This explains why, in countries like France, a national pilot program testing alternative voting procedures, such as in the UK or Switzerland for example, could not be envisioned. It is the product of a social convention designed to balance off a conception of the republic, a construct of citizenship and a vision for social order.

As a social phenomenon, it is an original way of materializing the incarnation of a procedure whose gradual ritualization has come to mark the crossover from the secular world to the sacred one. This is quite visible in the French procedure which follows a dramatic narrative structure that elevates to the status of empowered citizen any walk-in to a polling station.

[4] The ballot box was adopted in France in 1848 for mechanical reasons when universal suffrage legislation for all citizens aged 21+ upped the total number of ballots from 250,000 to over 9,000,000. The ballot box then entered a process of gradual symbolization.

Vote casting breaks down into a sequence of physical 'rites of passage' that involve specific positive do's and negative don'ts. It is interesting to read Arnold Van Gennep's diagrams of rites of passage in light of Yves Deloye (2000:10). Van Gennep associates passage from one stage to another with a material dimension that incarnates it as a recurring symbology of birth [Be86]. The voting ritual is a cultural construct that meets a need for higher meaning in a young republic eager to assert its social and political legitimacy, as was France in the 18th century. Borrowing the terms in brackets from anthropology, we can apply this observation to consider the act of voting as a mystical "transition state" [Bo79], which effects transubstantiation of the voter during a "liminal phase".[5] Reinforced by the privacy of the voting booth introduced in 1913, the transition state is all the more necessary insofar as political science theory makes the Nation-State the sole source of all legitimate power instead of citizens as individuals. However, the Nation-State remains an abstract concept far removed from the people, which leaders have learned to mistrust. The voting ritual operates transmutation of the people into the Nation-State by extracting from each voter a sample of that sovereign nationhood. The preliminaries serve as a separation rite that mourn the citizen's present social status and put it to death.[6] They are prerequisite to the aggregation of ballots in the urn, after voters pass through the voting booth. The purpose of the rite is to quantify the political will of the citizenry. Thus it ends with a postliminal phase consisting of a one-for-one count of all the ballots that express the opinions of socially unequal and very dissimilar individuals and add up to the Voice of the Nation-State.

It is now easier to understand how online voting can directly aggresses the traditional republican perception of citizenship in a democracy which intensifies the citizen's moral duty to exercise his rights of citizenship; he owes society his vote in exchange for the freedom and protection it supplies. It operates by "stripping the citizen of all social, religious and cultural attributes" [Sc01:81], which involves measures to guarantee the sincerity of the vote the ritual serves to express.

From this, online voting becomes pure sacrilege because of its concern for the voter's convenience (i.e. voting from home at any hour), for more efficient use of time (by both citizens and the government) and above all, for the faith it shows in the voter's ability to make sincere choices in an environment he deems insecure.

4 The Voter Behind the Virtual Ballot Box

The political habits of French and European citizens today differ noticeably from those that evolved since the first ballot boxes came out. Among them, three are of major importance to the perception of citizenship in a democracy.

---

[5] Victor Tuner (1969) prefers "liminality" (from *limen*: doorstep) to describe the stage suggestive of "limbo". Van Gennep's three stags of rites of passage thus become Preliminary (Separation), Liminal and Post-Liminal (Reincorporation).

[6] Separation rites have strong religious connotations that recall Biblical quotes about access to heaven, e.g. "…how hard it is for them that trust in riches to enter the kingdom of God. It is easier for a camel to go through the eye of a needle, than for a rich man to enter into the kingdom of God." (Mark, 10:24-25).

The first consideration is our relationship to time and space. The relentless pressure on people for ever higher productivity and efficiency comes into conflict with a demand for greater availability that government is hard-pressed to satisfy. Moreover, the greater mobility that technology affords makes it increasingly difficult for some persons to be available, given the requirement for physical presence at the polling station.[7]

Second, the citizen's relationship to the Nation-State has evolved greatly in the past century. Paternalism petered out after the 1968 uprising, as did condescending attitudes toward women. The proliferation of procedures for concerted action and public debate in numerous fields of civil and political activity[8] confirm recognition of the need for more two-way information flow between elected officials and voters as well as between experts and laymen. In line with Tom Janoski, I see the expansion of "active" political rights[9] as a noteworthy trend in modern democracies that perceive citizens as dialogue partners rather than just electors. By raising the French Republic to a sacred symbol of our common will to live together, the voting ritual clashes with recent developments that effectively reduce the symbolic distance between the citizens and their elected representatives.

However the most fundamental issue is what Ulrich Beck and Anthony Giddens call "reflexive modernization", which best explains the undermining of the three stages of the traditional voting ritual. It holds that the individual appropriates his social status as part of his personal identity but without perceiving that status as a determinant of his behaviour or lifestyle. Therefore, the physical isolation orchestrated for the liminal ritual to protect the citizen from indiscreet onlookers may be out of step with the perceived experience of voting. Many voters find that ritual isolation feels unnatural, especially in deliberative situations where individuals are valued for the unique worldviews endowed by their social positions [Yo99][10]. From this standpoint, reflexive modernity explains the trend whereby the individual who is accustomed to the rules of modern democracy becomes an agent for social change and appropriates the determinants bearing down upon him. The condescension and guilting (i.e. the citizen needs protection against himself and might be wanting to influencing others) of the liminal ritual seem out of step with the political practices of today's modern democracies.

The citizen of the digital era no longer fits the image foisted upon him by the traditional voting procedure. From this standpoint, the gradual erosion of the ritual induced by recourse to voting machines and online elections in Switzerland and elsewhere, ties in with a will to redefine citizenship, which needs new forms of materialization and post-modern rituals. It is therefore important to consider as a whole all the technological

---

[7] - In many countries, proxy voting is subject to strict requirements. Applicants must present at the defense ministry police (Gendarmerie), justify their absence on election day and the proxy must be a resident of the same voting district as the applicant, a condition harder to meet in larger urban agglomerations.

[8] - The theory of deliberative democracy which refers to a specific form of participation through discussion has played a determinant role in the development of such procedures. Among a huge academic literature, see Barber, 2003.

[9]- "Political rights refer to the right of participation in the public arena and are largely procedural, but the content of legislation is not usually part of political rights themselves" (1998:30).

[10]- Yves Deloye (1993) thus outlines various personal strategies to avoid the isolation of the voting booth by voters who feel they can make their choice discreetly without it.

constraints and models of citizenship in a debate that includes all players in the public arena. Some scholars have mapped out new definitions of citizenship in a digital era ([Cm01], [Ho99]) and have tried to link them with new ICT tools offered by local or national authorities. These models nevertheless tend to be driven by a deterministic approach to technology: they either associate new categories of citizenship with specific type of e-tools [Cm01], or build up a new citizenship : the digital one [Ho99]. Inspired by Janoski (1998) and Benjamin Barber (2003), I suggest in the table below to link the evolution of the conception of citizenship (from passive to more "active" and participative rights, [Ja98]) with their actual usage in modern democracies. This table suggests relationships to primary type of decision-making involved with a selection of their new materializations[11].

Model	**Administrative**	**Referendum**	**Republican**	**Deliberative**
Citizenship Concept	Systemic: citizens are numbers protected by a legal arsenal	Liberal: citizens are autonomous and wary of government	Republican: citizens are bound by a system of shared values. Strong integration: citizens are deferential towards government	Neo-Social:[12] Various corporate bodies involved in the government decision-making process
Relationship to Decision-Making	Action taken on applications with or without input from ad hoc commission(s)	Action taken after national referendum	Action taken after broad, legally non-binding consultation(s) with citizens	Action taken after due, legally-binding deliberations
Technology	E-government, Internet protocols, up/downloads and secure online payment	E-voting, E-referendums and Fishkin-type polling	Forums, gateway websites, public debates, conferences	Dedicated websites, online debates, etc.

Figure 1: Categories of Citizenship and their actual usage in modern democracies

Of course, these are weberian ideal-type models of citizenship and could not be found in their "pureness" form in modern states. One could nevertheless acknowledge trends in European or Northern American politics toward specific forms of citizenship by concentrating a national public effort on some of these technologies.

In most European countries for example, important public funds have been dedicated to on-line administrative services to the detriment of e-democracy procedures such as on-line consultations or public forums.

[11]- For an earlier version of this table, see [Mo03].
[12]- Janoski terms this "social or expansive democracy" while Barber calls it "strong democracy", see [Ja98].

This reveals the tendency of our political systems to reduce effectively the conception of citizenship to its administrative dimension rather than its participative one, even if the political discourse often underlines the need for more citizen's involvement in politics [Co01], [Co05a].

As such, electronic voting procedures correlate with conflicting perceptions of citizenship ranging from right-wing to neo-left-wing. However, the hybrid procedures for public debate sooner match a communitarian/republican or embryonic deliberative model. Thus, the new materializations offer a range of competing models of citizenship that combine to favour new ways of exploiting existing technologies. This two-way flow of creativity that broadens scope for grassroots participation assumes the creation of new rituals as well as a reframing of the role of existing rituals. The actual scholar discussion about the concept of "direct representation" [Co05b] correspond to this phase of conceptualisation which follows grassroots participative systems locally developed.

5 Conclusion

The introduction of new voting procedures requires a rethink of the relevance of the symbolism of the pre-existing procedures. To reduce consideration to purely technological, ergonomic or political issues will hardly map out the creative trends now witnessed in the ways in which citizens participate in the political decision-making processes, whether we are speaking of online voting or deliberative procedures. I also feel it is as important to maximize the social dimension of the new technologies used in the political process in order to take account of the major changes they impose on the materialization of our practices.

Our political systems and theoretical models are contingent upon the social practices that ritualize, symbolize and give meaning to them. To map out their development, researchers must set aside any norms about the "best system", which would skew observation of change in political practices. Recent field research and observation of new deliberative practices now yields a hypothesis for a trend into a new model of more deliberative citizenship [Ba03], [Co01], [Co05b]. Public confrontation between two opposing models with radically different consequences provides an opportunity to debate openly the role and future of the citizen in a modern democracy. Such debate would attest to the vitality of the social fabric and should not ignore the materialization of the citizen's voice, failing which discussion would focus only on technical issues. If so, we risk suffering the consequences, especially the symbolic ones.

References

[Ba03] Barber, B.: Strong democracy : Participatory Politics for a New Age. Berkeley: University of California Press, 2003 [1984].

[Be86] Belmont, N. : La notion de rite de passage , in Centlivres, P., Hainard, J., Les rites de passage aujourd'hui. Actes du colloque de Neufchâtel, 1981, Lausanne :L'age d'homme, 1986 ; pp. 9-19.

[Bo79] Bon, F. : Qu'est-ce qu'un vote ? , Histoire, n°2, 1986 ; pp.105-121.

[CM01] Chadwick, A., May, C. : Interaction between states and citizens in the age of Internet : 'e-government in the United States, Britain and the European Union, Annual Meeting of the American Political Science association, San Francisco, 2001.
[Co01] Coleman, S. : The transformation of citizenship ?, in Axford, B., Huggins, R. (eds.) New Media and Politics, London: Sage, 2001; pp.109-126.
[Co02] Coleman, S. (ed): Elections in the 21st Century: From Paper Ballot to E-Voting. Report by Commission on Alternative Voting Methods. London: Electoral Reform Society.
[Co05a] Coleman, S.: Direct Representation. Toward a Conversational Democracy. IPPR exchange, 2005.
[Co05b] Coleman, S. : New mediation and direct representation, reconceptualizing representation in the digital age, New Media and Society, Vol.7(2), 2005 ; pp.177-198.
[De93] Deloye, Y. : L'élection au village. Le geste électoral à l'occasion des scrutins cantonaux et régionaux de mars 1992 », Revue Française de Science Politique, Vol.43 n°1, 1993, pp.83-106.
[De98] Deloye, Y. : Rituel et symbolisme électoraux : réflexions sur l'expérience française », in Romanelli (ed.) How did they become voters ? The history of franchise in modern european representation. La Haye, Kluwer Law International, 1998 ; pp.53-76.
[Ho99] Hoff, J. : Towards a theory of Democracy for the information age , Discussion paper for the Democracy Platform UK-Nordic Meeting, 1999 .
[Ih93] Ihl, O: L'urne électorale, Revue Française Science Politique, Vol.43 n°1, 1993; p.30-60.
[Ja98] Janoski, T.: Citizenship and Civil Society, Cambridge University Press, 1998.
[KLS04] Kersting, N., Leenes, R., Svensson, J. : Adopting Electronic Voting. Context Matters" in Kersting, N., Baldersheim H. (eds), Electronic Voting and Democracy. A Comparative Analysis. London: Palgrave Macmillan, 2004.
[Le05] Ledun, M. : La démocratie assistée par ordinateur. Du sujet politique au consommateurs à caractère politique, Paris :Edition Connaissance et Savoirs, 2005.
[MM02] Maigret, E., Monnoyer-Smith, L. : Le vote en ligne : Nouvelles techniques, nouveaux citoyens ? », Réseaux, n°114, 2002.
http://www.utc.fr/costech/v2/pages/ch_publications.php?id=12
[Mo02a] Monnoyer-Smith, L. : Scenario on electronic citizenship. A roadmap for 2010", First EVE International Conference : E-democracy : scenarios for 2001. Paris, 2002.
[Mo02b] Monnoyer-Smith, L. : Review on electronic voting". First EVE International Conference E-democracy : scenarios for 2001, 2002.
[Mo03] Monnoyer-Smith, L. : Les enjeux inexprimés du vote électronique, Sciences de la Société, n°62, 2003 ; pp. 127-146.
[No04] Norris, P. : Electoral Engineering: Voting Rules and Political Behavior. Cambridge, Cambridge University Press, 2004.
[No05] Norris, P. : Internet voting and democratic politics in an age of crisis", in Trechsel A. (ed.) The European Union And E-voting: Addressing The European Parliament's Internet Voting Challenge, London: Routledge, 2005; pp.223-237.
[OV04] Oostveen, A., Van den Besselaar, P. : Internet voting technologies and civic participation, the users perspective. Javnost / The Public Vol. XI , No.1, 2004; pp.61-78.
[Sa01] Sassi, S. : The transformation of the public sphere ?, in B. Axford and R.Huggins (eds) New Media and Politics, London: Sage, 2001, pp.89-108.
[Sc00] Schnapper, D. : Qu'est ce que la citoyenneté ?, Paris : Gallimard, 2000.
[TM05] Trechsel, A., Mendez, F. : The European Union And E-voting. Addressing The European Parliament's Internet Voting Challenge, London: Routledge, 2005.
[Ts00] Tsagarrousianou, R. : Electronic democracy in practice…One , two, three…countless variants, Hermès n°26-27, 2000; pp.233-246.
[Va91] Van Gennep, A. : Les rites de passage, Paris: Editions Picard, 1991 [1909].
[Yo99] Young, I.M. : Difference as a resource for democratic communication", in J. Bohman and W. Rehg (eds) Deliberative democracy, Cambridge: MIT Press, 1999.

Session 3: Legal and Democratic Issues of E-Voting

The electoral legislation of the Basque autonomous community regarding electronic vote*

Rosa Mª Fernández[1], Esther González[2], José Manuel Vera[2]

[1]Departamento de Derecho Constitucional
Universidad Complutense de Madrid
Ciudad Universitaria s/n
28040, Madrid, Spain
ferrosa@der.ucm.es

[2]Departamento de Derecho Constitucional
Universidad Rey Juan Carlos
Paseo de los Artilleros, s/n
28032, Madrid, Spain
{esther.gonzalez | josemanuel.vera}@urjc.es

Abstract: The Basque Autonomous Community constitutes the only Spanish experience of legal electronic vote regulation. The Basque Government decided, by means of a government bill that was voted in its legislative Chamber on June of 1998, to reform its electoral law and insert, as possible option, an electronic vote by means of a magnetic strip card. This Law, which has not been applied yet, presents a series of important changes and of potential modifications in the Basque electoral system and, perhaps, in the Spanish system. At the same time, in the year 2004, a new government Bill of the Basque autonomous Community is presented in which an electronic vote legal regulation is once again presented. The news regarding the previous project are important. Its processing is interrupted by the dissolution of the Chamber and the new Government formation that, still today, has not retaken up this initiative. The electronic vote in "Euskadi" is a regulated normative topic but that has not yet been utilized in an electoral procedure with binding character.

1 Introduction

Norberto Bobbio indicated that the consolidation and the reinforcement of the democracy are indispensable budget for the transformation of society. For this, the consolidation of all institutions that allow maximum participation to the organs that are attributed with the collective power to make decisions in different levels and the maximum control on the correct execution of the decisions taken is indispensable.

* Work developed under project "Conceptos y sistemas de apoyo a la democracia electrónica" (EDEMOCRACIA-CM,S-0505/TIC/0230)

Deciding is somewhat indispensable for history process, for the development of public powers, for the concreteness of ideas, whatever their type and nature are. The Basque's Parliament decided, in 1998, to incorporate in its electoral law of 1990, a Chapter destined to the electronic vote. This legal regulation was produced like a first and onlyone, in the Spanish electoral system. The general context in which it was devised, so much in a cultural, economic, social, and political perspective, as a legal perspective (Spanish Constitution, constitutional law of General electoral State, etc.) means the object of analysis of this work. The burst of what are called New Technologies has supposed, among others many things, the availability of technological instruments at the service of citizens and of the parliament for exercise of their respective rights to vote.

2 Legal regulation of electronic vote in the Basque autonomous region.

2.1 Basque electoral law 15/1998, of 19th of June

On 9th July, 1998 the Law 15/1998 of 19th of June is published in the Basque Country Official Bulletin which reforms the Law 5/1990 of 15th of June regarding the Basque Parliament elections.

Its EXPOSITION OF MOTIVES expresses, in its second section, that any democratic society should guarantee the participation of its citizens in elections, by which it proceeds to the election of its representatives by means of secret, direct, equal, free, and universal vote. The full exercise of the right to vote requires that, next to traditional manners, new procedures be articulated that allow voters to emit the vote on the electoral polling station, of simple and personal form. The objective that the electronic vote pursues is to allow the articulation of a new form of participation of the citizens in the res publica.

1. Elements of the electronic vote.

The article with which Chapter X begins enumerates the elements that are included in the electronic vote system: magnetic card voting with magnetic strip; electronic ballot box; vote screen; voting booth and software or electoral data processing programs.

2. Organs and distribution of competencies regarding electronic vote material.

In first place, reference is made to the central electoral Committee of Basque Autonomous Community has following competences:

1. Approving the operation validity of the electoral software in magnetic support. This supposes that the data processing program should be validly prepared for the opening and closing of the voting, for the reading of the voting cards with its respective magnetic strips, for the control of the number of cards placed in the ballot box, for the final scrutiny of respective polling station and for the final broadcast of electoral results. Also the software validated in each polling station should be approved, this is, that it collects the necessary information relating to the concrete identification of the polling station, just as is indicated in the following number.

2. Devising the personalization of polling station's software.

3. Guaranteeing the availability and delivery of the software to the electoral Committee of Zone and to the polling station.

4. Receiving, once the elections have been finalized, the magnetic backups of the software and to assure their subsequent destruction.

5. Other functions that the law, or the relative dispositions to the software, entrust it. In second place, the law awards the electoral boards of Historic Territory, the competence to approve the validity of the software "specifications" that will be determined by the Basque Government by means of the Royal Decree. The Royal Decree that, at the same time, will set the characteristics of the booths, models, printing conditions, and making and delivery of the electoral documentation (art. 132 bis IV, 1, second paragraph).

In third place, and for the making and distribution of the cards with magnetic strip, of the electoral documentation and of any other necessary element to the electoral boards of Zone, the Government will be exclusively competent through their home office (art. 132 bis IV, 1). It will also be their competence to assure the availability and delivery of the electronic ballot box, the screen to vote and the voting booth, in each one of the respective electoral polling station.

Finally, the law clarifies that for the development of the functions described the aid of the data processing Service of the Basque Parliament will be included, as a support and advice organ, that it will even be able to participate with voice, but without vote, in the meetings of the electoral boards of Historic Territory or of the electoral board of the CAPV (Basque Autonomous County)

With the new electronic vote, the aid that the data processing Service should lend to the electoral organs in the fulfilment and development of its tasks is indispensable.

Therefore, important technical know-how is required. It is enough to remember that the first task attributed to the electoral board of the CAPV is "to approve the validity of the operation of the software (...)"; or the possibility that the art. 132 twice III, 4, establishes "(...) the general representative of each proclaimed candidacy, by itself or by means of an expert representative in data processing named by it, will be able to obtain, with prior character to its final approval, information on the correct operation of the software from the electoral board of the autonomous region (...)"; articles which doubt who now really passes control over the development of the electoral process. The question that arises regarding this would not be what organ is legitimized by the law to do it, but who is truly qualified for it[1].

3. Regarding the right to vote.

The article 132 ter refers to the "material means and operations prior to voting".

The law sets the need that in each polling station there are two ballot boxes: an electronic one and a traditional one to be able to place, in this one, the absentee ballot, that will be carried out by means of envelopes and ballots. Besides a voting booth will be necessary, or in its absence, a space reserved that allows the voter to be isolated. Both, cabin or space should be equipped with a screen for voting.

3.1 Secrecy in the exercise of the right to vote.

The obligatory character offered by law to the material means that the cabin or space reserved for the voter represents is important. The article 132 quater, I, 2 thus confirms it: "(...) the voter should enter the voting booth and introduce the card with voting magnetic strip in the screen (...)". From this it can be deduced that the electronic vote is "obligatorily secret", in its exercise.

On the contrary, the LOREG (Electoral, General and Organic Bil) article 86.2 determines "(...) the voters will approach the polling station one by one, after to have passed, if thus they desired it, by the cabin that will be placed in the same room, in an intermediate place between the entrance and the polling station (...)" and the article 104.2 of the Law of 1990 of Basque Parliament elections expresses in the following words: "The voter will be able to pass, if desired, by the cabin, collect the ballot of the chosen candidacy, introduce it in an envelope and proceed to voting". Both norms also consider the existence of voting booths obligatory, but these will be able to be or not be utilized by the voters in the exercise of their vote. What evidently strikes an important qualitative difference.

---

[1] "Now, it is certain that the establishment of the electronic vote, be it for periodic elections, be it for referendum consultations, strikes an essential problem of control of the process, that passes from the hands of the electoral boards (legal guarantee), of the citizens and of the representatives of the parties (political guarantee), to be protected by the data processing technicians, with serious the risk that the control be transferred, from the democratic environment to the technocratic stronghold. ..", Pau i Vall, *Democracia e Internet*, Yearbook of Parliamentary and Constitutional Right, Regional Assembly of Murcia, Nº 10, 1998

The different regulation of the secret character of the vote in the three legal norms stirs up the debate around its obligatory character or, on the contrary, its optional disposition to the will of the voter.

The Basque law introduces, with the electronic vote, a vote that is obligatorily secret[2] by demand of the procedure (the screen could have been placed out of the cabin or reserved space), what does not seem to be the same thing than out of courtesy of the constitutional mandate (art. 68.1 CE) the one that describes a secret vote without entering subsequent procedures relating to its execution or its put in practice.

The Constituent consecrated a secret vote, a characteristic not available for the legislator, and no too for the voter. Any legal regulation, or instrument contained in it regarding this characteristic of secrecy, (that embodies the nature of the vote in the Spanish State, along with others cited in the art. 68.1 CE), allow or enable its "availability", will be a clear constitutional breach. Can the universal character of the vote be arranged, deciding to restrict this to certain social collectives? Could it be decided perhaps as more convenient, that only an individual of each household voted for all of its members? Could we be able to accept, for example and for determined people, (businessmen, intellectuals, institutional heads ...) the concession of more than one vote? Evidently, for these cases the respective answers should be equally forceful. The universal character of the Vote is not available, its personal character is not available (existing only exceptional suppositions and valued by a legislator, in which the motive of the exception has had to be fully justified), and the constitutional recognition of the equality of the Vote is not available. The German doctrine is pronounced very clearly. Thus Karl-Heinz Seifers indicates in a comment to the federal electoral Law that "condition sine qua non of a free vote, is a secret vote". In turn, Reinhold Zippelius declares that the basic substrate of the secret vote is to guarantee the free vote. Each citizen has to be able to vote, with the safety that nobody is going to see or interfere in what has been voted. He should always voted without pressures nor alien influences, and Martin Morlok explains that the protection of the secret vote neutralizes social potential power and permits decisions or votes independent from forces or social achievements[3].

---

[2] We also can verify this pretension of the legislator to guarantee a secret exercise in the exercise of the electronic vote in the final Annex of definitions. In it is the definition of what is a voting booth: "A reserved precinct in which the voting screen is placed, in order to preserve the privacy of the vote by the voter".

[3] H. Buchstein, *Präsenzwahl, Briefwahl, Onlinewahl und der Grundsatz der geheimen Stimmabgabe,* page 898-899, *Zeitschrift für Parlamentsfragen*, Zparl. 4, Dezember 2000. The principle of secret vote, just as recognized in the constitutional law art. 38 GG, is not somewhat optional, but a legal obligation for all those who desire to take part in an electoral process. Any harm to this principle will be punishable with liberty deprivation of to two years, or with the equivalent pecuniary sanction (*Paragraph* 107c, Which title is: "*Verletzung des Wahlgeheimnisses*", *Strafgesetzbuch 23rd January, 1974,* modified *BGBl 58/200*); Zittel,T., Elektronische Demokratie: ein Demokratietypus der Zukunft, Seitschrift für Parlamentsfragen, Zparl. 4, Dezember 2000.

3.2 Anomalies in the exercise of voting.

Continuing with the development of the procedure, it is also possible that anomalies in its course be produced (art. 132 quater, III, 1 and 2). In that case, the law indicates that "(...) it will require the presence of the responsible person for the maintenance of the electronic vote material appointed to such effect so that, once the situation is analysed, and the opinion of the referred technician is heard, the President decides if the voting can continue, while the problem is rectified or, on the contrary, to interrupt the voting. .."

Once more, the importance of the necessary technical presence that conditions, if not replaces, the decision of the polling station's President is thus manifested[4].

It can also occur that the voting be interrupted and, in that case, the electronic ballot box must be "resumed", later, operations of emptying and extracting the cards with magnetic strip that have been placed in until to that moment should be carried out and that should be registered again in the hands, logically, of the members of the Polling station.

If the failure is not general, but affects only a voter that cannot register their vote in the magnetic card by means of an adequate use of the screen to vote, the law resolves this supposition with two requirements. In first place, the destruction of the voting magnetic card and, in second place, the delivery of another new validated card, to repeat the operation.

4. Counting time and following operations.

When the electronic process enters the counting phase, article 132 quinques, I and II, in first place, it defines what should be understood as a null vote and a blank vote. And, once the voting time has concluded, the President of the polling station reads the results aloud.

The section III, 5 of the article above mentioned categorically prohibits the possibility to communicate the results obtained, on the part of the electoral Polling stations, to the mainframe computer, before having finalized the counting.

The law also obliges, when the counting has finished, the recovery (for their subsequent erasing and possible reuse) of all the cards with magnetic strips, the ones that are found inside the electronic ballot box, as well as the ones that, by diverse motives, are found out of it (132 quinques, V, 2).

---

[4] GRAY BUESO, J.B., "Democracy and Technocracy: regarding the electronic vote", Parliamentary Magazine of the Assembly of Madrid, no. 3rd June 2000, pp. 64 and ss: "Now well, without denying the functional potentialities that new technologies suppose for the speculative and productive processes and for the dimension of the human knowledge, the movement of these sophisticated technologies to the political process of decision making, should be critically received and established with due cautions, with the shame of converting what could be valid instrumental elements, in any case helpful, in the media and conditioning that end up subverting capital principles of the constitutional system of government and the order of values *insito* to every political democracy".

5. Infractions and Sanctions.

Basic aims of the law are: security, transparency, credibility of this new procedure, simplicity, rapidity, modernity and privacy. In this way, the article 132 sexies enumerates diverse infractions regarding the vote, behaviours that, in some way, undermine those objectives:

a) Voluntary physical or mechanical manipulation of technical elements or of the electronic instruments (vgr. of the screen, of the magnetic cards...).
b) Alteration of the software which is used to count at the polling station.
c) Production, distribution, commercialization and unlawful use of magnetic cards.
d) Destruction of cards during the voting or the counting, with the exception of the cases that thus demand it.
e) Replacement of the magnetic card delivered by the President of the polling station, with a different one, that alters the correct operation.
f) To leave the electoral localities with a magnetic card without authorization.
g) The execution of the counting of the polling station in the case of having suspended the voting.

Chapter X concludes with article 132 septies, titled "Last dispositions". Continued an Annex is enclosed where a series of definitions regarding electronic vote are enumerated.

What deficiencies do the current Right of vote of the Spanish citizen present?

a) The "voting booth" model as a means to guarantee the secrecy of the vote.
b) The complexity and high price of a ballot per each candidacy

Currently, the printing price of the "infinite" candidacies is very high. The possibility of a unique ballot would suppose an important reduction of the expense[5]. It is true that the ballot would be able to contain only the name and symbol of the different political parties whose candidacies have been proclaimed and, at most, the first candidate of the list, what without doubt would imply certain changes for the voter that could not know now, by means of the ballot, is who forms part and in what order is each candidacy presented.

c) The problems derived from the elaboration and updating of the Electoral Census, especially of the CERA, Electoral Census of Absent Residents; furthermore, the numerous problems that the vote through correspondence implies.
d) The present availability regarding the secret character of the Right of vote bears an important interference of this right.

[5] For example, the ballots manufactured for the Elections of June (municipal and European) of 1999 cost 5,776,309 Euros, to what the figure of 2,029,583 Euros was added in concept of printing and envelopes. All of this keeping in mind that the mailing of the parties is credited to them as "electoral expenses", http://www.mir.es/derecho/procelec/loreg/6.htm.

2.2 The new government Bill of 2004

a.1) Exposition of motives and general justification of the new government Bill
Several ideas are explaining in the Exposition of motives of this new normative Text. In all a certain change on behalf of the legislator in his general reflections on the so called New Technologies is appreciated, probably derived from the multiple experiences that this Community has carried out in this matter[6].

1. The apparition of certain prudence or distrust regarding the utilization and application of New Technologies.
2. The perception of two languages and different frameworks, with norms of different operation: the technological framework and the framework of values and democratic principles.
3. The need of a "gradual application" of the New Technologies to the operation and development of democracy. The procedure of electronic vote tries a "sweet" application of the new technologies to the electoral processes. The Basque citizens are going to find a form of exercising the right to vote that, maintaining its characteristic elements, allows, nevertheless, the operation and application of the technologies, and at the same time is perceived without effort by the voter.
4. The conviction that New Technologies are an instrument, not a panacea, and as such should be at the service of "democratic principles".
5. The convenience of maintaining the traditional or classic system of envelops and ballots with the system of the electronic vote.

a.2) Description of the new electronic vote system
The new Chapter X of the government Bill of 2004 begins referring to the elements of the new system of electronic vote that are: a) the voting ballot, b) the electronic ballot box, c) the opening control cards and closing of the ballot box and d) the voting ballots verifying machine (art. 132 bis I).

The ballots, that will have certain resemblance to the classical ballots, will be able to be folded and to be closed. In the internal face of the ballot, the denomination, acronyms and symbols of the corresponding candidacy will be printed.

---

[6]The professor E. Arnaldo Alcubilla indicates that absentee ballots are a voting modality that exempts the presenting of the voter to the polling station the day of the elections, whose recognition, which still presents doubts, very poignantly from a point of view of the personality and secrecy of the vote principles, is based on the enlargement and facilitation of the participation of the electorate and, consequently, of the right of the voters with physical or professionals impediments that cannot attend on the day of the elections to vote personally, Arnaldo Alcubilla, E., "Considerations on the Reform of the electoral Law regarding absentee ballot", in *Reflexiones sobre el Régimen Electoral General*, IV Conference of Parliamentary Right, Congress of the Representatives, Madrid 1993, pp. 711 and ss. The Royal Mint, National Factory of Currency and Stamp, carried out in the year 2002 an electronic vote study for the Absent Residents, VERA system (Electronic Vote for Absent Residents) that has never been applied.
[6] Demotek, (2004) The electronic vote in the Basque Region, electoral processes and documentation direction / Home Office Department www.euskadi.net/botoelek/euskadi/antecedentes-c.htm [12th January 2004].

Likewise, the important novelty that such ballots introduce will be the so called "window of recognition" that appears in the external face of the ballot and that permits: "(…) the identification of the candidacy and other electoral options of electronic form and that can be verified by the voter" (art. 132 bis II. 1).

The function that the window of recognition performs is key in the development of the vote. The counting is carried out, in strict sense, through the window of recognition. In it, the individual electoral information of each voter is contained. "The information contained in the window of recognition will be able to be read with total reliability and security by the reader of the electronic ballot box machine. The electronic vote system fully guarantees the liberty of emission of the vote and the secrecy and counting of the vote" (art. 132 bis. IV).

The electoral Committee, that of the autonomous region as well as those of the Historic Territory, continue being responsible for guaranteeing the transparency and objectivity of the voting procedures and counting in the electoral polling station. For this they can include the support and contribution of the data processing Service of the Basque Parliament.

It also takes into consideration, to a certain extent, the voters that vote by mail and thus the law indicates (article 132 bis VII, 7): "The Government will adopt the opportune measures to guarantee that all the voters, included the absentee ballots, have an egalitarian deal that allows them to verify the chosen option in the window of recognition of the ballot".

In turn, regarding the voting exercise, we can identify the following steps to observe for the voter. 1.- Selection by the voter, inside the cabin, of the chosen voting ballot. With relation to this way of proceeding we should underline that, same as text of 1998, the secrecy of the vote is guaranteed, since thus is arranged to stop being an option. 2.- Verification of the ballot in the "verifying machine" that will read the window of recognition. 3.- The final close and fold of the ballot and its transfer to the electoral polling station. 4.- Delivery of the closed ballot to President of the polling station. 5.- Reading by the electronic ballot box of the ballot.

The procedure can continue from two alternative options: a) that the electronic ballot box, after the reading of the ballot, accepts it or b) that the electronic ballot box rejects the ballot, for different motives, after having performed its reading. In the first case, the shutter of the ballot box will be opened automatically and the President will place the ballot in it, increasing automatically the number of votes that figure on the screen. In the second supposition, the President will return the ballot to the voter inviting him to repeat the observed procedure.

If the vote has been registered correctly the Law establishes that the directors and, in its case the Administrators that desire it, will make a numbered list of the name and the surnames of the voters by order in which they have emitted their vote expressing the number with which they figure on the list of the electoral census. Every voter will have the right to examine if their name and surnames have been written correctly on the numbered list of voters that forms the polling station" (art. 132 quáter I. 4. and 5).

The wording that this new text offers is curious for what should be understood as "supposed accreditation" of the voter; this is done after the reading by the ballot box of the ballot, if this procedure can be identified as such[7], and all this it in spite of the great flexibility with which has always been acted in relation to accreditation of the voter. The Jurisprudence thus confirms it in sentences as that of the Supreme Court of Justice of Navarra of Dec. 4th, 1989, relating to the acceptance of a university card as valid id document or the of the Justice Supreme Court of Catalonia of December 4, 1989 decision that accepted, in similar terms, the copy of the National Document of Identity.

Many are questions that stir up regarding this since in no case is it the prior accreditation required before the polling station of the voter with the opportune documents to the effect. The voter votes before its data is verified (articles 85 and 86.3 of the LOREG), what occurs if after having voter voted and having his/her vote been registered by the electronic ballot box as valid, he/she is not found in the list of the electoral census that the members of the polling station have? We can find ourselves with a voter that may decide to cast their right to vote more than once.

Thus, unless the diligence that is presumed of the members of the polling station, has been truly such, and even then, (article 132 quarter II. 4: "If during the procedure of voting, the members of the polling station observe ill faith on the part of the voter at the moment of voting again with new ballots, the President will take the measures that it reckon convenient to impede actions that hinder the normal development of the voting") we can assure a correct development of the process.

---

[7] The Basque Parliament elections Law 5/1990, of 15th of June, article 105, reformed by Law 15/1998, of 19th June, by Law 6/200, of 4th October and by Law 1/2003, of 28 of March, establishes: "1. The right to vote will be accredited through the inscription in the certified copies of the Census lists or by the specific census certification and, in both cases, by the demonstration of the identity of the voter, that National Document of Identity will be carried out by means of Passport or driving Permit in which the photography of the holder appears. 2. The voters will only be able to vote once. The voting will be carried out in the Section and within the polling station that corresponds, with exception of the Administrators that only they will be able to vote on the polling station in which they exercise their functions. **3. The certified copies of the electoral census lists to which section 1 of this article refers to, will exclusively contain the voters of legal age on the date of voting.** 4. Furthermore, those who accredit their right to be recorded in the Census of the Section by means of the exhibition of the corresponding judicial sentence will be able to vote." Likewise, article 86.3 of the LOREG indicates: "Each voter will declare his/her name and surnames to the President. The Directors and Administrators will verify, by examining the electoral census lists or of the contributed certifications, the right to vote of the voter, as well as his/her identity which will be justified according to what is established in the previous article. Immediately, the voter will deliver the closed voting envelope or envelopes from his/her own hand to the President. Subsequently, the president, without hiding them at any moment from the public, will say the name of the voter aloud, and adding "Votes" will place the corresponding envelopes in the ballot box or ballot boxes.
Also curious is the Agreement of the Central electoral board of March 7th, 2000, regarding "the flexibility regarding the identification of the voters of Las Palmas and Tenerife, given that on Saturday 11 of March is the last festive day of the carnival in the Canaries and it is possible that the voters attend the ballot boxes with attires that be not habitual": "Without damage of the application of the legal precepts and interpretive criteria of this Council as for the identification of the voters and of the necessary seriousness of the electoral act, the polling stations should act with the flexibility advised by the circumstance to be March 12th, piñata Sunday, which refers to the attires with which the voters could attend with".

The problem would be produced, in any case, as a consequence that it be prior to the introduction of the ballot, properly manipulated[8], in the electronic ballot box without having to verify the census data on behalf of the members of the polling station, at least thus is how it is read as articulated.Subsequently, the President returns the "faulty" ballot to the voter and he invites the voter to elect a new one and to repeat the process of voting.

Finally, the 2004 text, object of our study, strike in its surprising article 132 quinques I: "1. There is not a ballot with the option of a null vote. 2. The electoral boards of Historic Territory will resolve the validity of the ballots reserved by the polling station in the cases predicted in the articles 132 quáter VII and 132 quinques VI. 3 of the present Law, being able to declare the nullity of the vote in the following supposition: a) When the vote is emitted in different a ballot from the official model. b) When the ballots contain, in its exterior, insults, expressions alien to the vote, signs of recognition or any another type of substantial alteration. c) When the absentee ballot contains more than one ballot per different candidacy. If there it was an envelope of vote by correspondence with more than one ballot of the same candidacy will be computed as a single vote".

Lastly, the article 132 quinques II regarding the blank vote indicates: "1. Blank votes will be those that: a) Are emitted in electronic ballot with the option of blank vote. b) are emitted in electronic ballot of a candidacy legally retreated of the electoral district. 2.- In spite of what is indicated in section 1.b), in the electronic counting of the polling station, the votes casting in favour of a candidacy legally retreated will be computed to such retreated candidacy and of the same form will figure in the Minutes of Session of the polling station. Subsequently, in the general counting, the electoral board of Historic Territory will consider such votes as blank votes.

a.3) The counting

Once the voting is concluded, the text of 2004, strikes two counting possibilities. Or the electronic counting, that is carries out provided that there were no problems and is done through the opportune manipulations of the electronic ballot box (art. 132 quinques IV, V), or what is called electronic-manual counting.

1.- In what circumstances can this type of electronic-manual scrutiny be performed?
This type of counting is only feasible when the polling station decides, by the majority, to accept the protests or claims presented against the result of the electronic counting that has been carried out.

Thus, the President will take note of the turn out and re-count the contained ballots in the ballot box the electronic-manual way. We would be before a closer recount mechanism species to a classical recount, what causes greater doses of civic confidence. The greater simplicity and comprehension on behalf of the voter of any of the operations and of their development, the greater confidence and sensation of security they have.

---

[8] Article 132 *quáter* II. 2 and 3: "If for any reason the voter's ballot is rejected by the electronic machine of the ballot box, the President of the Polling station at that moment will return the faulty ballot to the voter and he will invite him/her to elect a new voting ballot. The President of the Polling station should verify that the closed voting ballot that he receives from the voter does not contain, in its exterior, expressions alien to the vote or signs of recognition, or any other type of substantial alteration. In this case, the President will not admit this ballot and he will invite the voter to vote again".

2.- What does this type of counting consist of?
The article 132 quinques VI, describes it in detail. The recount only will be performed by the verifying machine located in the voting booth and that should be transferred at the polling station. In no case will it be permitted to open the ballots of electronic voting to avoid their possible deterioration and the consequent annulment of votes that have been emitted as valid. The process begins with the opening of the ballot box by the President of the polling station who will carry this out in the presence of the remainder of members. He will extract all the ballots of the electronic ballot box and he will pass them out one by one by the tester apparatus for the sake of a new reading on the screen.

3 Some desirable recommendations[9].

When we speak of new Technologies applied to the right of vote we mix two very different frameworks, with very different languages and characteristics. Now, the electronic vote, a formula that results from exercising the right of vote by means of instruments from such New Technologies or electronic Technologies should arise under a possible sole plan that is the one that our Legal Code designs and permits.

Our right of public participation through the direct, equal, free, universal and secret vote should remain fully guaranteed and only thus will we be able to try to implement an electronic vote destined, at every moment, to improve or to perfect the regulation of our present electoral vote.

1. Any regulation on electronic vote should part from its nature as "instrument" to the service of our Right to Vote.
2. To undertake a replacement of the present system of voting with envelopes and ballots, the advantages and benefits that the new proposed type of voting would contribute should be sufficiently accredited, and be possible in our legal system.
3. Any reform should part from the identification and faithful diagnosis of the present reality. The instrument should be designed from existing deficiencies and needs to try to alleviate them or rectify them.
4. Any reception of a new instrument should be done under the full knowledge[10] of the intended and not intended nature, characteristics and effects from it that could be derived.

---

[9] We furthermore refer to the Recommendations that the Council of Europe has elaborated regarding electronic vote, *Council of Europe* (2004) *Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical standards for e-enabled voting (IP1-S-EE), Integrated Project 1 –Making Democratic Institutions Work, IP1 (2004).*

[10] The full knowledge, inescapably, carries out experimental tests that are capable of offering data for the reflection and analysis. Thus, for example, we know that recently the present Government has approved a new pilot experience, this time of a national scope, of electronic vote, without legal efficacy, for 52 different municipalities, one for each one of the Spanish provinces during the referendum for the voting of the European Constitution on 20th of February. The Home Office will select the localities in function of its representatives and the sample of citizens that are able to emit their vote electronically will revolve around the two million voters, this is, 6% of the census approximately. Observatory-eDemocracia, 10/2005, (www.edemocracia.es)

5. Finally, we should mention that the potential that the New Technologies contain does not turn out to be at all contemptible. Any democracy should be benefited of these new tools, but we do not want to build a giant with clay feet. It is necessary to take the steps in an orderly fashion, with a parallel analysis of price-benefit that at times will advise us not to adopt a determined position or a determined mechanism.

We finish with a reference that professor Aguiar de Luque offers us, which is the future of democracy in an time in which the information and communication technologies redesign the places where politics unfold, borders are broken down, limits of space and time overflow and old type of discourse is annulled creating a new a subjectivity? If this it is the effect of change, it is not only a private model that is in effect, it is the society in its entirety that day by day is being transformed by these named new technologies[11].

References

[Al98] Alcubilla A. y D'Ambrosio i Gomáriz A., El voto electrónico: algunas experiencias recientes, Cuadernos de Derecho Público nº 4, mayo-agosto, 1998.

[As97] Assemblèe Parlementaire du Conseil de l'Europe de 22 de avril de 1997.

[Bu00] Buchstein H., Präsenzwahl, Briefwahl, Onlinewahl und der Grundsatz der Geheimen Stimmabgabe, Zeitschrift für Parlamentsfragen, Zparl. 4, Dezember 2000

[Ca00] Cano Bueso J. B., Democracia y tecnocracia: a propósito del voto electrónico, Revista Parlamentaria de la Asamblea de Madrid, Nº 3, junio 2000.

[Ca99] Carter M., Speaking Up in the internet age: Use and Value of Constituent E-mail and Congressional Web-sites, Democracy, Parliament in the age of the internet, Parliamentary Affairs, v. 52, nº 3, july 1999

[Do00] Doug Brown, Is virtual voting ready for real time?, ZDNet News, January 2000.

[Fi95] Fishkin J., Democracia y deliberación. Nuevas perspectivas para la reforma democrática, Ariel, Barcelona 1995.

[No99] Noam E., Why Information Technology is Bad for democracy, American Associaation for Public Opinion Research, Media studies Center 1999.

[Pa98] Pau i Vall F., Democracia e Internet, Anuario de Derecho Constitucional y Parlamentario, Asamblea Regional de Murcia/Universidad de Murcia, nº 10 1998.

[Pa99] Pau i Vall F. y Sánchez i Pycaniol J., Democracia y nuevas Tecnologías, VI Jornadas de la Asociación española de Letrados de Parlamentos autonómicos, Pamplona 1999.

[Sa99] Sánchez Muñoz O., Sistema electoral y principio de igualdad de sufragio, VI Jornadas de la Asociación española de Letrados de Parlamentos autonómicos, Pamplona 1999.

[Sa97] Sánchez Navarro A. J., Telemática y democracia, en José Asensi Sabater (coord.), Ciudadano e Instituciones en el Constitucionalismo actual, Tirant lo Blanch, Valencia 1997.

[St99] Strassman M., Internet Voting Circa 2002, Intellectual/Capitol.com, May 1999.

[Zi00] Zittel T., Elektronische Demokratie: ein Demokratietypus der Zukunft, Zeitschrift für Parlamentsfragen, Zparl. 4, Dezember 2000

[11] Aguiar de Luque, L. "El impacto de las Nuevas Tecnologías sobre el principio representativo", in II Madrid's Assembly Parliamentary Conference, Parliament and New Technologies, Madrid, October 2001, pp. 27 and ss.

E-Voting in Brazil - The Risks to Democracy

José Rodrigues-Filho, Cynthia J. Alexander, and Luciano C. Batista

Federal University of Paraiba, Paraiba, Brazil and
Acadia University, Nova Scotia, Canada
jrodrigues-filho@uol.com.br
cynthia.alexander@acadiau.ca
luciano@lbatista.com.br

Abstract: Literature has shown that countries with strong democratic traditions, such as the United States and Canada, are not yet using electronic voting systems intensively, due to the concern for and emphasis on security. It has revealed that there is no such thing as an error-free computer system, let alone an electronic voting system, and that existing technology does not offer the conditions necessary for a reliable, accurate and secure electronic voting system. In this context, then, what are the risks of e-voting to democracy? In what ways, if at all, can more fragile, less mature democracies be buttressed with e-voting systems? As a key component of e-democracy, it seems that e-voting technologies are to become more secure and increasingly reliable in the near future and will indeed be adopted in many countries. In what ways, if at all, will the introduction of such systems increase voter confidence in the political system, promote citizen engagement in political life, and nurture the evolution of democracy? If both e-voting and e-democracy are emerging based on popular demand - that is, as a demand-driven alternative to current processes, then there is no doubt that they are likely to enhance and improve the efficiency of traditional democracy. However, if e-voting technology is being introduced based on a supply-driven fashion - the technology exists therefore it should and must be implemented - then the implications for democracy should be considered. Brazil's introduction of e-voting offers a cautionary tale of supply-driven technological implication. The purpose of this paper is to demonstrate how the introduction of e-voting in Brazil is highly risky to democracy due to the lack of emphasis on security and the lack of a socially-informed and socially driven approach to technological innovation. The Brazilian example illustrates the democratic implications of a market-driven approach. The lack of a technology strategy designed to promote and extend democratic principles is not surprising given the closed door, market-based negotiations that led to the adoption of e-voting in Brazil. The promise, and indeed, the imperative of a democratic, voter-centered approach as an alternative for the development of an electronic voting system, is explored in the paper.

1 Introduction

Literature has shown that countries with strong democratic traditions are not yet using electronic voting systems intensively, given citizens' and policy makers' concerns about the security of such systems. To date, commercially available technology requires an infrastructure that poses complex technical challenges for reliability and security. Despite our technological process, e-voting technology does not yet provide a completely "secure e-transaction environment" [XM04]. Some authors claim that e-voting will never be error-free [Mo04] and that it is nice in theory [OB04], but that in practice, the risks are too large.

Given the lack of security of e-voting systems, what are the risks of e-voting to democracy when the systems are introduced? Can more fragile, less mature democracies such as those in Latin America, be reinforced and advanced with the adoption of e-voting systems? Indeed, what are the implications for emerging democracies when e-elections engage millions of poor people, many of whom live well-below the poverty line? What are the implications of this costly 'technological imperative' upon the policy priorities of their governments? The contradictions are apparent: most countries in the developed world have held off adopting e-voting systems given their concerns about security and their knowledge of the implications of insecure systems for democracy.

However, costly technological systems are being imposed on citizens in less developed countries, where questions about voting abnormalities can go far beyond the scandal of hanging or 'dimpled' chads discovered and heatedly contested in the 2000 Presidential Election in the United States. Which criteria or benefits justify a full-scale electronic election, when the costs - budgetary, democratic and other - are so high? What are the implications when a public network project is conceived and implemented in the interests of corporate actors without consideration for the needs and interests of millions of illiterate people unaccustomed to even traditional voting methods, let alone electronic systems? In what ways, if at all, might an e-voting strategy be conceived which serves the democratic vision of citizens in less developed countries? These and many other questions have not been posed, let alone addressed.

In Brazil, investments in information technology and other e-government initiatives, such as e-voting, have been evolving without a definition of an appropriate information and communication technologies (ICTs) strategy; there has been scant public policy analysis and little academic research work that assesses the heavy public sector investments in ICTs. Surprisingly, there has been no public sector or academic evaluation of e-voting in Brazil, even in places in which there are claims of tampering in the voting process. There is a need to initiate the discussion about e-voting in Brazil to determine whether the country should continue its e-voting initiative, given the significant resources that have been allocated to carry out electronic elections, and given that the initiative has been driven by market push rather than by the electoral needs and interests of the citizenry.

The Superior Electoral Court (Tribunal Superior Eleitoral – TSE), known as the Electoral Justice, is responsible for election administration in Brazil; it has unexpectedly and rapidly adopted a technological system that has not yet been sufficiently tested even in the developed world. The controversies over e-voting are under way and e-voting technological failures have been documented. More recently, scientists started to worry about computer voting systems and numerous reports have found them vulnerable to errors and tampering [OB04, Ko03, Ha03, Ko03, Ma03].

Previous research work, using data related to expenditures in information technology, compiled from the Electoral Justice, has recognized that investments in e-voting are higher than those allocated to basic social programs which serve the needs of the poor much more effectively, in policy fields ranging from education to health. Consequently, e-voting in Brazil seems to reinforce the digital divide and undermine democracy [RG06].

Democracy depends on healthy and educated citizenship; if technology can further policy objectives around education, health and well-being, then indeed, the investment in innovation can be defended in a less developed country. However, when a market-driven approach dominates, the adoption of technology for technology's sake, without due consideration and strategic efforts to mitigate the foreseen and unintended side effects of technological adoption, then there is an obligation to question the motivation for such an initiative, to assess the implications of the adoption of technology, and to push for public dialogue about the relevance and appropriateness of the current course of action.

If a socially-driven technology strategy were in place, the infusion of technology into the public sector might well serve the needs of citizens, particularly those living at the political, economic and cultural margins of society. This strategy should be one that harnesses the power of technology to enhance the design and delivery of health care through tele-health services such as those being introduced to meet the needs of Canada's northern indigenous peoples, or to support innovation in education through the development of culturally appropriate e-learning initiatives that would meet the needs of rural and remote communities as has been the case with the evolution of the Alaskan Native Knowledge Network in the past decade. Such examples of technological investments might encourage democratic dividends, and serve as important enablers that allow at-risk individuals and communities to participate effectively as citizens and as productive contributors to the local and national economy.

The purpose of this paper is to demonstrate how the introduction of e-voting in Brazil is highly risky to democracy due to the lack of emphasis on security and the lack of a socially-informed and socially driven approach to technological innovation. Brazil was the first country in the world to conduct the biggest election on the planet using e-voting technologies. In 2002, more than 100 million voters cast their ballots on more than 406,000 touch-screen machines scattered all over the biggest country in South America.

The paper provides insight into the imperative of moving away from the user-centered to a citizen-centered approach for the design and development of an electronic voting system. In this empowering or enabling approach, people are viewed as subjects who seek to deepen democracy and not as objects, users or customers. Within a top-down decision-making approach, the needs of the market dominate the user-centered approach and results in aggravating existing inequalities. In this sense, what we can see now in many discussions held by the information society is the user-centered model as an ideal to consider the needs of the people, when, in reality, this model means the use, and abuse, of the user of the system.

2 E-voting Insecurity in Brazil

Literature has shown that, to date, commercially available technology requires an infrastructure that poses complex technical challenges for reliability and security. In short, e-voting technology does not provide a completely "secure e-transaction environment" [XM04]. It is also claimed that e-voting will never be error-free [Mo04] and that it is nice in theory [OB04], but that in practice, the risks are too large. Consequently, what the literature has shown is that there seems to be an emergent consensus that existing technology does not sufficiently attend the principles of computer security. In this case, software can be modified in such a way that the results of an election can be modified, with it being very difficult to be detected [Fi03].

Despite the rather intense debate on the idea of e-voting, literature has shown that countries with a strong democratic tradition are not yet using electronic voting systems intensively, due to their emphasis on security. We understand that both democracy and voting are processes much more complex than its electronic version and a secure voting system in itself is a basic element of a true democracy. The question here is: Why has Brazil started using e-voting technology so early in the evolution of the technological systems, when the country does not possess the domain of this technology? The answer is quite simple. The e-voting project in Brazil is based on a rather technical and reductionist view that neglects both the social and political aspects of e-voting. The implementation of e-voting, under the state and corporate governance, is a project by the current dominant networks towards the commercialization and depoliticalization of ICT that can jeopardize democracy. A market-driven approach appears apolitical; technology is perceived as a value-neutral system that can readily deliver efficiency gains within the democratic market-place. The e-voting technology deployed in Brazil is a direct recording electronic (DRE) voting system; it has been judged by Brazilian experts as being more vulnerable to tampering than any another voting system. For some electronic voting experts, the Electoral Justice has opened the doors for new and sophisticated fraud, more serious than the traditional kind [Ma00, MJ02].

In the developed world, the concerns about direct record electronic (DRE) voting technology are not different. Many reports in the United States articulate the risks of this technology, corroborating with what Brazilian academics and scientists say [TCM04, Ko03]. In the U.S, the controversies over e-voting are not stifled; e-voting technological failures have been registered all over.

More recently, scientists started to worry about computer voting systems and numerous reports have found them vulnerable to errors and tampering [OB04, Ko03, Ha03, Ma03]. Given the stakes, any facet of e-democracy, from e-policy consultations to e-voting, needs to be well-researched. Premature investments in e-voting systems are financially, and democratically, irresponsible.

3 Market-Driven Approach to E-voting

Appropriate technological approaches lost favor in the 1980s under U.S. President Ronald Reagan's administration. The neo-liberal agenda privileges economic efficiency, an objective that the informatics sector has fed in the past twenty-five years. There has been a heavy predisposition in governments, in the developed and developing world, to ignore the socio-political and cultural implications of ICTs.

Technological determinism seems to have prevailed in the decisions to introduce electronic voting in Brazil. Because of this, the nightmares of the electronic dreams have already started to appear, even without a deep discussion within a social vision of the technology, which would be enough to put electronic voting in its right place. A recent study carried out by the Organization for Economic and Development Cooperation (OECD) confirms that, if governments do not learn how to manage the risks of information technology, the electronic dreams will become global nightmares [OEC01].

There is a need to expand the discussion about e-voting in Brazil in order to see whether the country needs an electronic voting system or not, considering that investments in e-voting are higher than that in basic social programs that could help the poor much more in the areas of education and health [RG06]. If people knew how high the cost of e-voting technology is in Brazil, many of them might consider it an expensive toy belonging to the rich and privileged. E-voting systems require a heavy investment in both infrastructure and services, posing serious opportunity-cost evaluation and prioritization. Brazil is confronted with many pressing domestic demands and competing priorities from healthcare, to water and sewage quality to housing and education needs.

Unfortunately, critical questions revolving around conceptions, implementation, maintenance, affordability, and evaluation of possible consequences of implementing e-voting on values, economy, context and politics were not discussed with the Brazilian academy and society as a whole. Will e-voting empower the ordinary people? Will e-voting enhance the opportunities of the poor and illiterate to vote without coercion? Will e-voting avoid vote selling? Or, if e-voting technology is not discussed with the society, will it strengthen the powers of the elites, the rich, the educated and the corporate actors at the expense of the ordinary people? It has already been mentioned that e-voting in Brazil has contributed to reinforce the digital divide [RG06].

Therefore, in the Brazilian context, e-voting investments are more in the ICT than in social development for the protection of the disadvantaged and underprivileged groups. The investments in e-voting are higher than investments in important social projects like the control and prevention of cancer, teaching hospitals to attend the poor and the program of income and employment generation [RG06]. There is no doubt that the technological capabilities for the adoption of e-voting will exist in the near future. It is known that many good initiatives of e-democracy and e-government are operational in many advanced rich countries. But these are countries that are not only rich and highly industrialized, they also have had a vast experience in democracy and good governance. .

When access to clean water and food are questionable, raising the idea of investing heavily in e-voting systems is laughable not laudable. Electronic voting should not be considered a priority for people lacking food, health care and clean water. Before thinking about e-voting and e-Brazil, the availability of all services in traditional, non-electronic format, should be guaranteed to everyone.

The discourse of e-democracy has to be reframed beyond the dominant and mainstream rhetoric, so that the political aspects of ICTs meet the real needs of the 'democratic deficit', disclosing the true promises of technology. The high costs of an electronic election can reinforce the digital divide in the sense that it does not reduce inequalities in access to technology, especially when access is created by market-driven forces or corporate actors and the vote is compulsory. On the other hand, in an environment in which corruption in the election process is not an abstract thing, e-voting can appear to jeopardize democracy. The praxis of e-voting must encompass the issues of e-equity, justice and social inclusion.

4 Voter-Centered Approach to E-voting

It is extremely difficult to develop advanced computer applications to support complex human tasks. In the rational design approach, which is still predominant, computer designers too often use models and concepts that focus on the artefact without paying attention to the context in which the artefact is used. However, during the last years, the importance of context is emphasized in the design of computer tools, applications and systems – the context of using and the context of designing computer artefacts. Consequently, in the close relationship between design and use, it was possible to bring together various computing-related research disciplines, such as information systems (IS), human-computer interaction (HCI), computer-supported cooperative work (CSCW), and software engineering, as well as those social science disciplines that are also concerned with the theory and practice of the design and use of computer artefacts [KM97].

In this work we point out the limitations of viewing computer systems as a tool, as in the case of some HCI-research, in which the user-tool-task model is used. Although user-centered design is advocated in the Human Computer Interaction (HCI) literature, it is not as widely practiced as its proponents believe is necessary [GK91]. It has been claimed that from its inception, HCI has been closely aligned with the modernist program, whereby technology has been objectified, reduced, and 'black-boxed'. The participatory tradition has emphasized that this perspective is more likely to favour executives' workplace perspectives over those of low-status workers [KM97, GK91, SN93, BEK87].

In order to be useful to software professionals, HCI workers are often called upon to simplify the users' world and world-view - to make the users' complex experiences conform to the language of requirements analysis and software engineering, constructing fixed requirements from the ambiguous, exploratory, diverse, and mutable world of the users. In some views of HCI and requirements analysis, there is a tradition of reducing complex concepts to simple relationships, as the users' world is represented in the software developers' domain [Mu04].

On the other hand, one should consider many factors related to the problem being addressed or solved by the system, because the conditions may be used to move the software professionals closer to the users or to move the users closer to the software professionals ("move whom to whom"), creating a reference language [Mu04]. In this way, the recent studies on usability with regard to e-voting systems should be considered as very relevant [BHN03, La04], considering that this new technology should not be used as it is proposed now. In the case of Brazil, there is a need for this kind of study in order to show how poor or elegant the voting machine is in the eyes of voters.

As the field of HCI moves towards a new paradigm of user-centered (rather than system- or programmer-centered) design, there will be expanded opportunities for social theorists to participate in the development of information systems. By drawing on this new HCI perspective, an attempt is made to use the user concept to the analogous concept of voter or citizen. This will be better elaborated and expanded as a base for the design of an electronic voting system, in which the voter or citizen can be seen as an emancipator or radical political agent.

The process of dialogue - the social construction of meaning – will be more complete and will be better informed if its process encourages all knowledgeable people to participate. People are more likely to participate and contribute if they feel that their interests are being represented, typically through a democratic process. They are more likely to criticize and correct the group's understanding through a democratic process that solicits and values the diverse voices of all interests. In this view, the processes of creation and negotiation require full participation [KM97].

If the voting process is an important component of democracy, the democratic system should call upon the voters to develop the most appropriate voting system. An election is always a fairly disorganized activity, and the voters have to discuss how to organize it better. In addition, it seems that in the near future, the democratic process can be enhanced by reliable and trustworthy electronic voting systems, created and negotiated by the voters. If there is hope for a voter-driven voting system development, any technology-driven or market-driven voting system should be seen with suspicion in a true democracy. This is the case in the traditional ones.

It has been mentioned that one major cause of system failures is the exclusion, from the design process, of people who will be using the system. When users are not involved in the development of systems like e-voting, democracy will be put in jeopardy [OB04]. Therefore, with regard to the development of an electronic voting system we should take a political stance explicitly and not just keep focusing on methods and techniques to allow more participation, as it often the case in the literature.

In this and future work, an attempt is being made to raise political issues with regard to the development of an electronic voting system, trying to develop an understanding of the manifestations of power relations in and through ICT and software, when the citizen is nearly forgotten. The history of e-voting in Brazil and all its power relations embedded in it has not yet been told. Attempts are being made to focus on the humanization of the electronic voting system in Brazil that needs to be developed under a more elaborated socio-political approach.

5 Conclusion

The democratic potential of information and communication technologies has been widely discussed in the literature since the 1970s, and dominated the discourse of policy makers in developed countries in the Eighties and Nineties, particularly with the explosion of the Internet Revolution in the mid-Nineties. The initial public discourse around the Information Highway in Canada and the United States began with national discussions about how to define access, and even, whether to see access to the Internet as a public good or public utility. It did not take long for the market to persuade governments that all that was needed were narrow-based definitions of ‘access’, focused on mere technological access rather than considerations of literacy and other factors. Even in developed countries such as Canada, the digital divide persists, keeping vulnerable communities such as Indigenous Peoples and African Nova Scotians at the margins of the Knowledge Society, and maintaining the historic economic marginalization of communities in remote or periphery regions such as Atlantic Canada or Nunavut.

Technology tends to take the path of least resistance. In developed countries, resistance to e-voting has been consistent. Without a market for e-voting systems in the developed world, corporate actors have turned to developing countries. Just as pharmaceutical companies whose drugs do not pass the Federal Drug Administration's criteria push their products in the developing world, so too have ICT corporations cast their market nets in the Southern hemisphere.

While Diebold, the electronic voting machine maker, is so questioned in the United States, in Brazil it has the largest contract in its history by selling e-voting machines to the Brazilian government. In a press release in January 2000, Procomp Amazonia Indústria Eletrônica, a subsidiary of Diebold, announced: "For Diebold, this is the largest single order in the company's 141-year history" [Di00]. Negotiating behind closed doors, without the need for public dialogue, it is not surprising that a voter-centered approach was not developed as an alternative for the development of an electronic voting system.

If both e-voting and e-democracy are conceived and adopted based on popular demand (demand-driven option), then the efficiency of traditional democratic electoral processes may be enhanced. However, if e-voting technology is introduced as a supply-driven operation, it is imperative to identify and assess the risks to democracy.

It seems that the introduction of e-voting in Brazil has been risky business. Democracy is at stake. Health and social welfare are on the line, subject to cutbacks despite growing needs. Technology has dominated and driven the policy agenda. Technological hubris and market imperatives have driven the evolution of the Digital Society, with important democratic implications. Appropriate technological processes can reverse this trend in a way that ensures that we are not travelling along the path of least resistance.

References

[BHN03] Bederson, B.; Herrnson, P.; Niemi, R.: Electronic Voting Systems Usability Issues, CHI 2003, ACM Conference on Human Factors in Computing Systems, 5(1), 145-152, Florida: Ft. Lauderdale, 2003.

[BEK87] Bjerknes, G.; Ehn, P.; Kyng, M.: Computers and Democracy: A Scandinavian Challenge. Aldershot, UK: Avebury, 1987.

[Di00] Diebold – News Releases, 2000. Available online at http://www.diebold.com/news/newsdisp.asp?id=2636. Accessed on 25/09/2005.

[Fi03] Fischer, E.: Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. Congressional Research Service (CRS) Report for Congress, 2003.

[GK91] Greenbaum, J.; Kyng, M.: Design at Work: Cooperative design of computer systems. Hillsdale, NJ: Erlbaum, 1991.

[Ha03] Harris, B.: Black Box Voting: Vote Tampering in the 21 Century. Elon House/Plan Nine, 2003.

[Ko03] Kohno, T.; Stubbefield, A.; Ruvin, A.; Wallach, D.: Analysis of the Electronic Voting System. John Hopkins Information Security Institute. Technical Report TR-2003-19, July 23rd, 2003.

[Ko03] Konrad, R.: E-voting critics point to security hole. California primary results appeared online before polls closed. Associated Press MSNBC News, 2003. Available online at http://stacks.msnbc.com/news/964736.asp?0dm=n15ot. Accessed on 20/09/2005.

[KM97] Kyng, M.; Mathiassen, L.: Computers and Design in Context. The MIT Press, Massachusetts, 1997.

[La04] Laskowski, S.: Putting People First: The Importance of User-Centered Design and Universal Usability to Voting Systems. National Institute of Standards and Technology, Gaithersburg, MD, 2004. Available online at www7.nationalacademies.org/cstb/project_evoting_wq_sjl.pdf. Accessed on 30/09/2005.

[Ma00] Maneschy, O.: Fraude Eletrônica nas Eleições, 2000. Available online at http://www1.jus.com.br/doutrina/. Accessed on 10/01/2002.

[MJ02] Maneschy, O.; Jacobiskind, M.: Burla Eletrônica. Rio de Janeiro: Fundação Alberto Pasqualini, 2002.

[Ma03] Manjoo, F.: Hacking democracy?, 2003. Available online at http://www.salon.com/tech/feature/2003/02/20/voting_machine_standards. Accessed on 16/09/2005.

[Mo04] Moynihan, D.: Building Secure Elections: E-Voting, Security, and Systems Theory. Public Administration Review 64(5), 2004, pp. 515-528.

[Mu04] Muller, M.: HCI as Translation Work: How Translation Studies can Inform HCI Research and Practice. CHI Workshop on Reflexive HCI, 2004.

[OEC01] OECD: The Hidden Threat to E-Government: Avoiding Large Government IT Failures. PUMA Policy, 2001.

[OB04] Oostveen, A.; van den Besselaar, P.: Ask No Questions and Be Told No Lies. EICAR Conference CD-ROM, Copenhagen, 2004.

[RG06] Rodrigues-Filho, J., Gomes, N.: E-Voting in Brazil – Exacerbating Alienation and the Digital Divide. 6th European Conference on e-Government, Marburg, 2006.

[SN93] Schuler, D.; Namioka, A.: Participatory Design: Principles and Practices. Hillsdale, NJ, USA: Erlbaum, 1993.

[TCM04] The Caltech / MIT Voting Technology Project. Residual Votes Attributable to Technology – An assessment of the Reliability of Existing Voting Equipment, 2001. Available online at www.vote.caltech.edu/Reports/index.html. Accessed on 10.02.2004.

[XM04] Xenakis, A.; Macintosh, A.: Procedural Security in Electronic Voting. Proceedings of the 37th Hawai International Conference on Systems Sciences, 2004, pp.118a.

Session 4:
Analyzing Solutions for the Uncontrolled Environment

Multiple Casts in Online Voting: Analyzing Chances

Melanie Volkamer[1], Rüdiger Grimm[2]

[1]German Research Center for Artificial Intelligence (DFKI GmbH)
Stuhlsatzenhausweg 3
66123 Saarbrücken, Germany
volkamer@dfki.de

[2]Universität Koblenz-Landau
Universitätsstraße 1
56070 Koblenz, Germany
grimm@uni-koblenz.de

Abstract: We analyze multiple casts as an easy and non-technical approach to overcome some of the open questions and risks of online voting. The mechanism of multiple casts can be added to almost all existing online voting systems. Nevertheless, there are also some disadvantages, for instance the validity of a timestamp, which are discussed in the paper as well.

1 Introduction

Multiple casts in online voting became popular by the Estonian's legal binding Local Government Council Election in autumn 2005. The voters had the possibility to cast several electronic ballots from different places and devices before the election day. Only the last one was counted. In addition, the voter could cast a paper ballot in the polling station on the election day. In case a voter cast a paper ballot, this paper ballot was counted and any of his electronic ballots was deleted. The Estonian government applied multiple casts in online voting to overcome the discussion about remote voting like voter coercion and ballot buying, because in Estonia postal voting is currently only allowed for citizens living abroad.

The Estonian approach caused a controversial discussion in the (e-)voting community. Nevertheless, multiple casts in online voting is not a new approach, it is not even specific for online voting. Multiple casts in voting are already applied in some countries, e.g. in most of the Scandinavian countries, in the traditional voting system to limit the risks of remote voting in general and to overcome the problem that remote voters are early voters and could not response to short-term political events otherwise. Other reasons are the transmission time and the missing receipt within postal voting. For

instance, in Sweden the voters have the possibility to cast their vote in the polling station even if they already applied remote voting (postal voting or voting in a post office). The ballot cast in the polling station is counted and the remote ballot is deleted. The disadvantage of the Swedish approach is the long period to count the postal ballots because the electoral staffs have first to verify whether the voter cast a ballot in the polling station. With paper ballots, this check cannot be done automatically but it would be possible within online voting.

Thus, some countries have already recognized the advantages of multiple casts in voting. Why do we not utilize these advantages for online voting in general? Is it possible? Are there any other advantages or disadvantages? Does it overcome existing problems and open questions of online voting? To get an answer to all these questions we analyze multiple casts in online voting. We start with an introduction of security requirements and threats to an online voting system in section 2 and identify the open problems specific for online voting in section 3. In section 4 we present different forms of multiple casts in online voting. The advantages will be discussed in section 5 and the disadvantages in section 6. Besides the disadvantages, we will explain in section 7 those mechanisms and techniques, which are necessary to apply multiple casts in online voting. In addition, we will analyze the application with the existing voting systems and approaches in section 8. Finally, we will conclude with a summery and a recommendation for the application of multiple casts in online voting.

2 Requirements and Threats of Online Voting Systems

The main principles of election laws are similar in all democracies. Democratic elections have to be at least *universal, equal, free* and *secret*. Starting from these basic principles, many researchers deduced technical requirements for an online voting system and organisational requirements for the application of online voting. The most popular system and protocol independent requirement catalogues are the Recommendations of the Council of Europe [CoE04] and the Catalogue of Requirements for "Online Voting Systems for Nonparliamentary Elections" of the Physikalisch-Technische Bundesanstalt [PTB04]. These are the main technical requirements to an online voting system:

Deduced from the *universal* principle the election system must ensure that no eligible voter is excluded from the election - $\mathbf{Req_u}$. This must also hold for any kind of server or client software breakdown as well as communication breakdown. In addition, no voter has the possibility to cast more than one ballot within such a break down (equal). To ensure the *equality* principle, no unauthorized person should be able to add, remove or alter votes undetected. This must hold during ballot casting - $\mathbf{Req_{e1}}$, ballot transmission - $\mathbf{Req_{e2}}$ and ballot storage - $\mathbf{Req_{e3}}$. The principle of *secret* elections demands that only the voter is aware of her voting decision. Nobody else is able to link the voter to her vote neither during nor after the election - $\mathbf{Req_{s1}}$. In addition, voters must be unable to prove their voting decisions - $\mathbf{Req_{s2}}$. There are two more requirements, which are less technical but more general. The principle of free elections requires that voters cast their ballot free of duress and without influence - $\mathbf{Req_f}$. In addition, the principle of equal elections requires that all voters can cast their ballots in the same way - $\mathbf{Req_{e4}}$.

An attacker has four attacking points either in order to *break the ballot secrecy* (violation of the secret and free election principle) or to *manipulate the election result* (violation of the equal, free and universal election principle):

Observing a voter casting her ballot - The attacker could be next to the voter casting her ballot in order to observe the voters choice or to coerce her to vote in a specific way (e.g. imaginable in an old people's home) - $\mathbf{Threat_O}$. This is not an online voting specific attack but one for any remote voting system because the electoral office cannot ensure that voters cast their ballots in a free and secret environment. This is why postal voting is not allowed in many countries, and in some countries only as an exception.

Manipulation of the voters' voting device - The attacker could also program malicious code and try to install it on the voter's PC. This code could read the voter's ID, and vote on his behalf - $\mathbf{Threat_{D1}}$, or change the voter's choice before sending it to the electoral server - $\mathbf{Threat_{D2}}$. Moreover, attacking the voter's PC is much more critical than the observation attack from above because now it is possible to manipulate or read several votes automatically. Of course, this attacker needed technical expertise.

Manipulation or sniffing on the communication layer - The Internet is a public network so we cannot prevent an attacker to read or manipulate the connection between the voter and the electoral servers. The attacker can try to manipulate the election result by changing, adding or deleting ballot messages on the network - $\mathbf{Threat_M}$. He can also read and store messages in order to evaluate them - $\mathbf{Threat_S}$. The attacker could wait until someone will find a fast algorithm or faster PCs to decrypt the stored messages.

Manipulation of the election servers - The election servers store beside other data both information, the voters' IDs and their votes. Thus, an attacker could try to get access to the election servers in order to get the corresponding data - $\mathbf{Threat_{E1}}$. He could also try to manipulate the servers - $\mathbf{Threat_{E2}}$.

	$\mathbf{Req_u}$	$\mathbf{Req_{e1}}$	$\mathbf{Req_{e2}}$	$\mathbf{Req_{e3}}$	$\mathbf{Req_{s1}}$	$\mathbf{Req_{s2}}$	$\mathbf{Req_f}$
$\mathbf{Threat_O}$					x	x	x
$\mathbf{Threat_{D1}}$					x	x	x
$\mathbf{Threat_{D2}}$	x	x					
$\mathbf{Threat_M}$			x				
$\mathbf{Threat_S}$					x	x	x
$\mathbf{Threat_{ES1}}$					x	x	x
$\mathbf{Threat_{ES2}}$				x			

Figure 1: Comparison Requirements - Threats

The table in Figure 1 illustrates which threat violates which security requirement.

3 Open Problems

Many different approaches exist to overcome the threats above and to meet the identified requirements. For an overview over different approaches, see e.g. [Lip05, Sch00]. Most requirements are fulfilled by the existing online voting systems but some unsolved

problems exist nevertheless. Some open problems can be identified by **deduction from the identified threats**. Others stem from **functional requirements**, and from **voting in advance**. These are discussed in the following.

Problems deduced from the identified threats: Obviously, a remote online voting system does not overcome the observation problem - $\mathbf{Threat_O}$. As long as there is no technical or organizational approach to overcome this basic problem remote online voting will only be applied in parallel to postal voting - at least for important elections like parliamentary ones. The main technical challenge, which has not been solved yet, is the malicious code on the voter's PC - $\mathbf{Threat_{D1}}$, $\mathbf{Threat_{D2}}$. There are some approaches like the assistance guidelines for the voters within the elections of the Gesellschaft für Informatik [Gi05], and the theoretical approach of Fischer and Zuser [FiZu05] where the voter does not enter the original vote but a scrambled one. The disadvantages of the existing approaches are organizational assumptions and usability. Thus, a convincing solution to this problem is still missing. Another unsolved problem is the temporary unlimited election secrecy against attackers sniffing on the internet - $\mathbf{Threat_S}$. In [VoKr06] the authors illustrate that the election secrecy is only ensured under corresponding cryptographic assumptions. However, if someone finds a fast algorithm or if he has enough computational power he will be able to link each voter to her vote. The only possibility known so far to enforce theoretical information security with respect to the election secrecy and with respect to attacker sniffing on the Internet is the application of a One-Time-Pad. However, this implies a very high organizational investment.

Other open problems: One main problem in the context of online voting is to ensure that the voter can cast one and only one vote even when her local system, the communication system or the servers break down at any arbitrary step. This is a very important **functional requirement** in the context of online voting. It is hard to ensure this requirement because arbitrary things can happen, e.g. programming errors or an interruption of power supply or communication breakdowns. Another problem with respect to remote and especially postal voting is the **voting in advance**. In traditional postal voting without multiple casts, once the voter has cast her ballot, she cannot change her mind again for any reason, even if political events would cause her to do so. With online voting it is less a problem than within postal voting because the transmission time is much shorter. However, online voting would have problems to guarantee availability if everyone would cast the e-ballot on the Election Day, especially in the last few minutes before closing the election.

4 Forms of Multiple Casts in Online Voting

There are several possibilities to apply multiple casts in online voting which look similar on the first view. But from the organizational point of view they use different methods to ensure that multiple casts are counted only once even if voters use different channels: online voting, postal voting, and traditional voting in the polling station.

(a) The easiest form is to allow online voting exclusively, whereby voters can cast as many e-ballots as they want. *(b)*Within the second form, voters have to decide before the

election whether they want to use online voting or not. Here, a voter receives either a postal voting ballot or the electronic authentication tokens to access the online voting system. Thus, two different electoral registers exists: one for the traditional paper ballot voters and one for the e-voters. The e-voters can cast as many e-votes as they want and only the last one is counted. By doing so, it can be ensured easily that either an e-ballot or a paper ballot is counted.

(c) In the third variant, voters have the possibility to decide during the election time whether they want to apply online voting or not. After having cast an e-ballot the voter cannot cast a paper ballot anymore. But, she can cast as many e-ballots as she wants and the last one is counted. The possibility to apply online voting stops before the Election Day. An election register is printed for the Election Day, which lists all voters who did not cast an e-ballot. Listed voters are excluded from paper voting in the polling station. In addition, depending on the priority, either the e-ballot or the postal ballot has to be deleted to ensure that only one ballot per voter is counted. *(d)* Another possible form of multiple casts in online voting is an extension of (c). We allow voters to cast e-ballots also on the Election Day as long as they have not cast a paper ballot in the polling station. In this case, there is only one electoral register and we have to find a way to delete the e-ballots and/or the postal ballot. A more complicated form would be the following variant (d'): The voter can cast as many e-ballots as she wants, especially also on the Election Day and even *after* having cast a paper ballot. Here, the most favourite form of ballot casting (paper or e-ballot) has to be set up before the election, either uniformly for all voters, or even individually for every voter. For the calculation of the result, it must be possible to remove either the e-ballot or the paper ballot if someone cast ballots using both channels. In all cases it is important to delete the ballots without breaking or endangering the anonymity. Figure 2 illustrates the state machine of the described possibilities.

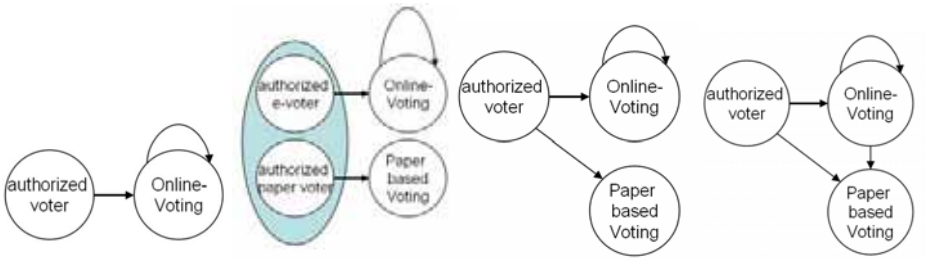

Figure 2: Forms of multiple casts in online voting

5 Advantages of Multiple Casts in Online Voting

Multiple casts in online voting provide a technical approach to overcome some of the open question especially the basic problems with respect to remote voting. The following advantages hold for all forms of multiple casts in online voting described above. First of all the principle of a free and secret ballot casting can be ensured also in the private sector - $\mathbf{Threat_O}$. Of course, an attacker can still observe and force the voter

to cast a ballot but the voter has the possibility to cast later on another ballot and to make another choice. So, it gets unattractive for an attacker to visit people in order to force them to cast a ballot. This is also true in old people's home because the attacker does not know whether someone else will go later on to the same old people's home and manipulate the voters to make another choice. Moreover, any voter who would like to change an unwanted vote could do so at any time. For the same reason, ballot buying gets unattractive[1].

Multiple casts in online voting can also be seen as an easy mechanism to ensure temporary unlimited election secrecy against an attacker sniffing on the Internet and trying to link identified voters to their votes after the election - $\mathbf{Threat_S}$. Strictly speaking, sniffing on the Internet becomes pointless for an attacker because in general he cannot know whether the last and counted ballot of a specific voter is in his memory of sniffed messages or not. The voter could have sent another ballot from another device and thereby over another path - a path on which the attacker is not sniffing. The sniffed encrypted ballots sent over the network become even less meaningful if the voting system allows an e-voter to substitute her e-ballot by a paper one - ***form (d)***. In the multiple casts form (d) an attacker can neither use the sniffed messages to break the election secrecy nor prove to someone else that the sniffed ballots represent valid votes of identified voters. Thus, the application of multiple casts in online voting makes the effort of sniffing and breaking encrypted ballots useless because attackers only get the counted ballots with a certain degree of (unknown) probability. Moreover they cannot use their knowledge to proof it to others.

Another advantage refers to manipulation attacks. When a voter would find out that she has malicious code on her PC during the election time, she is allowed to cast another ballot from an arbitrary PC or from special secure voting terminals or even on paper – $\mathbf{Threat_{D1}}$, $\mathbf{Threat_{D2}}$. With multiple cast, manipulation attacks are only meaning full with respect to result manipulation. The information from the malicious code cannot be used to break the election secrecy because the voter could cast later on another ballot from another device.

There exist two more advantages of multiple cast in online voting. First, the **mal functionality problem** with respect to system or communication breakdowns can be mitigated. If a voter does not receive a receipt at the end of the voting protocol because some problems arose, there is no reason to worry, because the voter can restart the PC, the software and/or the communication and cast her ballot again to get the receipt and to be sure that the ballot is counted. Second, multiple casts in online voting would also overcome the **voting in advanced problem**. A voter can change her ballot at any time at least until the Election Day if some political events happen or the voter has other reasons to change her mind.

[1] This is only true, it the system does not have a receipt mechanism with a zero-knowledge proof. The proof would change for a resubmitted vote and thus the coercer or vote-buyer would notice the resubmission. This does also hold for the temporary unlimited election secrecy in the next paragraph.

6 Disadvantages of Multiple Casts in Online Voting

This new type of voting system with multiple casts does not only have advantages but also some disadvantages. The disadvantages are not specific for online voting in general but for multiple casts in online voting. The main issue of concern refers to the requirement $\mathbf{Req_{e4}}$ that all voters must have the same chances to cast the ballot. *Form (a)* of multiple casts in online voting fulfils this requirement because only online voting is allowed. However, this form can only be applied if every voter has the possibility to cast a ballot (otherwise the universal election principle would be violated). The other proposed forms of multiple casts in online voting - *(b)-(d)* - do not comply with requirement $\mathbf{Req_{e4}}$. Here, the e-voters have the possibility to cast several votes and change their decision while people who are not able or do not have a PC and thus must apply the paper-based election, have only the possibility to cast one ballot. This is especially problematic with respect to the postal voters because they have to cast their vote some days in advance. Moreover, e-voters can get a receipt about the storage of their vote in the electronic ballot box but postal voters do not receive such a receipt. They are discriminated compared to the e-voters with respect to the equality principle.

Currently, at the end of the election most of the systems provide a consistency check. They compare the number of announced voters in the electronic voters register who finished their voting process with the number of votes stored in the ballot box server. This check helps to increase the trust in the system. With multiple casts in online voting, this check is much less meaningful. The voter could announce the vote several times to the electronic electoral register, which would label the voter after the first completed voting process. So, we do not get any statement about the multiple votes cast later on. This unveils another disadvantage of all forms of multiple casts in online voting: It is difficult to verify whether the one vote which is counted is indeed the vote the voter wants to be counted.

Some more disadvantages refer to social aspects: with multiple casts in online voting, we run the risk to loose the seriousness and the value of elections. It becomes similar to a game or some silly polls in the Internet or on TV. Closely related to this is the problem that some critical or unconfident voters could be unsettled which of their votes is actually counted. In addition, with multiple casts in online voting there might arise confusion with election forecasts. While in practise election forecasts are an important part of the election, they must be clearly separated from them.

7 Additional Mechanisms and Techniques

The existing systems have to be extended in order to apply multiple casts in online voting. Several auxiliary mechanisms are necessary and some new techniques have to be developed or have to be taken over from other applications. For example, it has to be ensured that the last cast ballot is the one that is stored and not e.g. the last ballot received at the ballot box. A challenging problem is the deletion of obsolescent ballots. The related function must either delete the e-ballots or destroy the paper ballots in order to allow multiple channel voting as described as ***forms (b), (c)*** and ***(d)***. Another important mechanism is the *timestamp* mechanism for the ballot messages. This becomes

necessary because multiple casts open the door to a new form of replay attacks. An attacker could send an older ballot again in order to manipulate the result. Reliable timestamps can only be provided by a trusted timeserver. The clock of the voter's PC would not suffice, because it is easy to manipulate it. Using the incoming time of a ballot at the ballot box server does not work either, because the ballot message could be withheld by an attacker and forwarded later. Thus, we need a possibility to uniquely assign a ballot message to the time when it was really cast by the voter.

The possibility to cast multiple ballots has to be integrated in the online voting system. There are two possibilities to implement this function. Either the voter's right to vote is checked in the electoral register each time she wants to cast a ballot or it is only verified the first time. In the latter case, the voter would receive an anonymous authentication token, which she uses each time she wants to cast a ballot during the election. Here, the voter needs to have a secure portable memory to store this token. Otherwise, she does not have the possibility to cast the ballot from arbitrary PCs. This could be a smart card, for instance. The problem is that the voter is excluded from casting ballots if this memory gets lost, stolen, or broken. In addition, high security requirements like integrity and confidentiality have to be ensured by the chosen memory otherwise the token could be read out. Therefore, the cheaper, easier and more user-friendly way is the first form: to run through the whole voting process each time again. This mechanism has to be implemented in all proposed forms of multiple casts in online voting.

In some forms of multiple casts in online voting, we have to integrate an additional and very critical mechanism. In ***forms (c)*** and ***(d)*** where the voter can cast both e-ballots and paper ballots the functionality to remove either the paper ballots or the e-ballots has to be implemented. There must be a link either between the e-ballot and the voter or between the paper ballot and the voter, or the voter must be able to remove one of them. This link must be possible without the violation of the secrecy principle (unlinkability forever). At least for the paper ballot election in the polling station the introduction of a link between voter and ballot would downgrade the anonymity compared to the traditional elections in the polling station. In particular for the e-ballots a technical solution must exist which does not violate the election secrecy. There must be a technical means to find the old e-ballot of the voter in the electronic ballot box in order to delete it and to store the new one. A possible solution is provided in [VoRV06].

In addition, the algorithm to replace the old ballot of a specific voter in the electronic ballot box by a new one must be fast. If the algorithm is too slow, the voter has to wait undue until she receives a receipt. ***form (d)*** of multiple casts in online voting requires two additional mechanisms: After the voter cast a paper ballot, the e-ballot has to be deleted and it must be ensured that the voter cannot cast an authorized e-ballot later on. Another mechanism should be implemented in each multiple cast form for online voting: *the wilful abstention from voting after having cast e-ballots*. This means: a voter who has already cast an e-ballot should be able to decide explicitly not to vote at all and thus her already cast ballot to be deleted and not counted. Thereby two things must be done: The ballot has to be secured in the ballot box and a corresponding flag in the voters' register has to be set.

8 Realization of Multiple Cast in Online Voting

There are three types of online voting approaches to overcome the anonymity problem: (1) preliminary voter authentication with subsequent anonymous tokens or pseudonyms, (2) blind signatures and (3) homomorphic encryption. In this chapter, we have a closer look whether multiple casts in online voting can be applied to all of these approaches and which are the respective protocol extensions or new assumptions.

Preliminary voter authentication means, that first the voter sends a request with personal data to the electoral register. This register generates an anonymous token and sends it back to the voter. Second, the voter sends her ballot together with the token to the electronic ballot box. The authentication of the cast ballot is checked by the eligibility of the token. Here it is quite easy to apply multiple casts in online voting because the electoral register just sends the same random token to the voter when she wants to announce a new vote. The ballot box can identify all ballots from one voter by the anonymous token. The difference to the implementation now is that the tokens cannot be deleted after having completed one voting procedure because they are needed for the multiple votes as well. Thus, the anonymity is more endangered and thus the servers have to be better protected. Another variant of preliminary voter authentication is pseudonymous voting. Here the application of multiple casts would be easier with less danger for the anonymity. But, generally, pseudonyms are harder to administrate.

Voting protocols with blind signature are based on Chaum's blind signature algorithm. Blind signatures allow to sign a vote or other data without revealing the content. There are two possibilities to apply this technology to voting protocols: firstly, the voters register blinds the ballot; alternatively, the voters register signs a blinded random token chosen by the voter. The latter one works perfectly with multiple casts in online voting. The random token is sent together with the ballot. Thus, the token can be used to identify all votes from one voter. The first approach to let the voters register blindly sign ballots does also work: currently the voter receives blinded ballots from the voters register for all possible choices. At present, the voter can only choose one of it and send it to the ballot box. With the same mechanism the ballot box now verifies that the voter only sends one of the signed ballots, the ballot box can identify the old ballot of a voter to remove this with the new one in multiple casts in online voting. Here, the application of multiple casts in online voting provides the same anonymity as online voting without multiple casts.

Voting protocols based on homomorphic encryption can also be extended quite easily because the link between an encrypted ballot and the voter is given and can even be proved. Thus, it is easy to replace an old ballot by a new one on the so-called bulletin board.

9 Conclusion

We have illustrated these open problems of online voting: observation within remote voting, manipulation of the voter's PC, the temporary unlimited election secrecy against sniffing on the network, the mal functionality with respect to system and communication breakdowns, and the voting in advance problems. Multiple casts in online voting overcomes some of these problems, namely obviously the remote problem, the voting in advance and the mal functionality problem. The manipulation of the PC is still a possibility for the attacker to manipulate the election result but not to break the election secrecy.

Beyond technology and organizational issues, we should also consider the voters themselves. Security increases only if the voters take the opportunity to cast several votes. Indeed, most of the voters will not do so. In Estonia, they counted 364 of 9681 repeated e-ballots and 30 of them cancelled e-ballots by casting a paper ballot on the Election Day. Therefore, it might be a nice, technically easy but only theoretical solution, which does not overcome the problems in practice. We should also take into account that changing electoral laws in order to allow online voting is not easy in general but it will be harder to allow multiple casts in online voting because multiple casts in voting is not in use in most of the countries. Moreover, there are also disadvantages like the integration of a trusted timeserver, the violation of the equal election with some forms of multiple casts in online voting, and the new mechanisms, which might be critical with respect to the election secrecy. We have identified some open research questions in this context, which have to be solved first.

References

[CoE04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation rec(2004)11 adopted by the committee of ministers of the council of europe and explanatory memorandum. Council of Europe, Straburg, 2004.

[FiZu05] Gerald Fischer and Wolfgang Zuser. The Vote Scrambling Algorithm. Schweighofer E., Augeneder, S., Liebwald, D., Menzel, T. - Boorbergverlag, 2005.

[Gi05] GI Gesellschaft f¨ur Informatik e.V. Election 2005 Assistance guidlines. http://www.gi-ev.de/wahlen2005/ retrieved on 15-2-2006, 2005.

[Lip05] Helger Lipmaa. Electronic voting. http://www.cs.ut.ee/ lipmaa/crypto/link/protocols/ voting.php retrieved on 15-2-2005.

[PTB04] Physikalisch-Technische Bundesanstalt Braunscheig PTB and Berlin. Online Voting Systems for Nonparliamentary Elections - Catalogue of Requirements. http://www. berlin.ptb.de/8/85/LB8 5 2004 1AnfKat.pdf retrieved on 15-2-2005, 8.5.2004.

[Sch00] Schlifni M. Electronic Voting Systems and Electronic Democracy: Participatory E-politics for a New Wave of Democrac. Dissertation Technische Universität Wien, 2000.

[VoKr06] Melanie Volkamer and Robert Krimmer. Secrecy forever? analysis of anonymity in internet-based voting protocols. In (not yet publish conference in April 2006), editor, The First International Conference on Availability, Reliability and Security; The International Dependability Conference Bridging Theory and Practice, 2006.

[VoRV05] Melanie Volkamer, Walter Reinhard, and Roland Vogt. Fuse - ein Internetwahlsystem für zeitlich unbegrenzte geheime Betriebsratswahlen. Sicherheit 2006 ”Sicherheit - Schutz und Zuverlässigkeit”, 22 February 2006.

How to create trust in electronic voting over an untrusted platform

Gerhard Skagestein[1], Are Vegard Haug[2], Einar Nødtvedt[3], Judith Rossebø[4]

[1]University of Oslo, Dept. of Informatics
Box 1080 Blindern, N-0316 Oslo, Norway
gerhard@ifi.uio.no

[2]University of Oslo, Dept. of Political Science
Box 1097 Blindern, N-0317 Oslo, Norway
a.v.haug@stv.uio.no

[3]Senit rådgivning AS
Skogtunet 12, N-1369 Stabekk, Norway
einar@senit.no

[4]Norwegian University of Science and Technology, Dept. of Telematics,
and Telenor R&D
Snarøyveien 30, N-1331 Fornebu, Norway
Judith.Rossebo@telenor.com

Abstract: Casting electronic votes via an inherently unreliable channel like the Internet in an uncontrolled environment is controversial for two main reasons: The first one is of democratic nature and the second of technical nature. The democratic concerns are about the possible dangers of buying and selling votes and so called "family voting". The technical concerns are how to convince everybody involved that the votes will be anonymously and accurately recorded and counted, and that no votes will get changed or lost, and that no "fake votes" will be introduced, with the knowledge that any computerized system may contain bugs or may be hacked by evildoers.

In this paper, we will show how the principle of repeated vote casting may be used to alleviate both the democratic and the technical concerns above, and how hybrid cryptography makes it possible for the voter to inspect his votes as stored within the voting system.

1 Introduction

In 2004, the Ministry of Local Government and Regional Development in Norway mandated a working group to work out a recommendation concerning the future of electronic elections in the country. The result of this work is documented in the report [KRD2006]. The basic conclusions are that there is no need to rush into electronic voting and that electronic solutions should be introduced with great care, due to the current deficiencies in the technical platform. Yet the working group recommended the setup of a project group and a step-by-step introduction of e-voting for certain types of elections. However, we do not know when the solutions proposed in this paper will be turned into reality, or whether they will be realised at all.

The working group rather quickly arrived at the conclusion that it had little value to put electronic solutions into the polling places – the ultimate goal had to be to give the voter the possibility to vote in uncontrolled environments from his home or at work. The particular solutions described in this paper is recommended as the basis for a possible system for Internet-voting in uncontrolled environments, as an alternative to solutions built on trustworthy platforms which may show up in the future.

The working group has been very well aware of the Recommendation No. R (2004) 11 of the Committee of Ministers to member states on E-voting [Rec2004] (later in this paper referred to as "the Recommendation"), and maintain the point of view that the proposed solutions are compatible with its intentions, although perhaps not always with its lettering.

Readers familiar with the Estonian electronic voting system [Maaten2004] [NEC2004] will find a lot of similarities. However, it may be of interest to know that the working group did arrive at similar principles before obtaining detailed knowledge about the Estonian system.

2 Two important principles

The solution proposed in this paper relies heavily on two fundamental principles: The principle of two-phase voting and the principle of repeated vote-casting.

2.1 The principle of two-phase voting

Elections in Norway have for a long time been carried out in two phases: One advanced voting phase followed by the Election Day itself. Between the two phases there is a one or two day break. During this period, the voters who have voted during the first phase will be marked in the Voter register, so that this information is available for the election officials on Election Day.

We propose to continue with this two-phase setup. Electronic voting should be used only in the first phase, voting on the Election Day should be done in the traditional way by means of paper ballots. This gives the voters complete freedom in how to vote, electronically or by paper ballots. At some time in the future, electronic voting may become so popular that the efforts for setting up traditional elections will be reduced to almost nothing. This is feasible; however, it will be driven by the preferences of the voters, the politicians and the society in general, not by the technology.

2.2 The principle of repeated vote-casting

The Recommendation [Rec2004], paragraphs 5 to 8, states the obvious democratic rule that a voter should give only one valid vote in each election event (one person – one vote). An electronic system may enforce this rule in two ways, either by invalidating the voter's credentials for further voting in the same election event, or by letting the vote-receiving server in some way keep track of the identity of the voter and reject multiple ballots from the same voter. The first solution is susceptible to conscious or unconscious errors and mistakes on the client side. Hence, it is better to let the server side handle the duplicate ballots from the same voter. We propose to let the vote-storage server store all the received ballots, rather than rejecting the second and the following ballots. At the end of the voting period, the election system will run through the ballots and only the last ballot received from each voter will be transferred to the electronic ballot box. Thus, the voter may effectively regret and cancel his vote just by casting another one at a later point in time.

As a final possibility for repeated vote-casting, the voter may show up on the Election Day asking to vote by means of a traditional paper ballot. In that case, the election officials will register with the vote-receiving server an instruction to throw away all the electronic ballots cast by the voter during phase one.

The principle of repeated vote-casting reduces significantly the well know democratic concerns connected with voting in uncontrolled environments [Maaten 2004]. There will be no market for buying and selling votes, since the buyer can never know whether the voter will cast another vote, maybe even on the Election Day. And the voter who feels subjected to coercion (e.g. "family voting") may cast another vote as soon as the coercer has disappeared. As we shall see, the principle also makes it possible to allow the voter to check the content of his electronic ballot as it is stored on the vote-storage server, since an observer can never know whether this ballot will be the final one.

3 Raising trust by securing the electronic voting system

Whenever communicating over an insecure channel, the demands for security must be built into the applications *using* the insecure channel. Basically, the sender may send a certain amount of redundant data with the message so that the receiver can check the consistency of the data and ask for retransmission if something seems to be wrong, or the receiver may reflect back to the sender its understanding of the message so that the sender can check that the receiver understood the message correctly.

The weakest point in an electronic election system based on voting in uncontrolled environments is probably the client machine, which may be infected by viruses and other malicious programs. The most difficult part to control is the very first part of the journey of a message from the keyboard to the program handling the input from the keyboard. We can not rule out the possibility that some illegal program is sitting between the keyboard and the rest of the system, faking correct looking screen images but sending completely incorrect data to the vote-receiving server. The only (almost) secure way to compensate for this threat is to have the user enter some redundant data via another completely separated and independent channel, for example via SMS on a mobile phone. The user friendliness in such a setup, however, is questionable.

It is more appealing to let the system reflect back to the voter so much data that the voter is convinced that the vote has been correctly registered. In this way, we utilise two different channels between the mind of the voter and the system: The typing on the keyboard and the visual observation of the reflected data on the screen.

It is, however, important that the reflection of the data is not done by an untrusted client machine, but by a trusted, well controlled server. In order to rule out the possibility that the client may intercept the reflected data and make it look right even if it isn't, the data may be returned to the voter via a completely different technical channel, for example SMS on a mobile phone.

The voting client in the system described in this paper is assumed to be a client machine. However, with the emergence of smartphones, GSM telephones equipped with WLAN access, 3G networks and more and more sophisticated mobile terminals, it is feasible that the voting client is a mobile handset. The advantage is that each of these is equipped with a GSM SIM card or a USIM card upon which the user's ID and PKI functions and key pair can be generated and safely contained. Note that in this case, access to the (U)SIM is secured by PIN and PUK, and the users private key never leaves the (U)SIM, see [THJ2004] for details regarding PKI on the (U)SIM.

3.1 The double envelope principle

In order to be able to allow recasting of votes, some kind of voter identity has to follow the ballot until the last, counting ballot is eventually dropped into the electronic ballot box. At the same time, in order to keep the vote secret, the identity of the voter and the content of the ballot must not be made available to anybody at any time. To ensure this, we propose to use an electronic double envelope setup similar to the one used in the Estonian election system [Maaten2004].

We employ two sets of key pairs for asymmetric cryptography. The first set consists of the public and private key of the voter[1]. The second set consists of the public and private key for the election event. In addition, we will also employ a session key in a symmetric cryptographic process.

As soon as the voter has finalized his electronic ballot and is ready to send it to the vote-receiving server, the client will generate a random session key and perform a symmetric encryption of the ballot. Then the session key is encrypted with the public key of the election event. The message consisting of the encrypted vote together with the encrypted session key corresponds to a paper ballot in a sealed inner envelope.

Normally, this two-step encryption process, called hybrid crypto, is used just for efficiency reasons, since symmetric crypto-algorithms are much quicker than the asymmetric ones. However, in our scheme, the hybrid crypto is also used for another purpose, as we will see.

Next, the client will digitally sign the message with the private key of the voter. This signed message corresponds to an outer envelope containing the already mentioned inner envelope. To the message, we attach some data which in some way gives the identity of the voter.

The whole package is then sent to the vote-receiving server, which will relay it to a firewall-protected vote-storage server where it will be written to a write-once-medium. Further ballots in double envelopes from the same voter will be written to the same medium, and not overwrite previous ballots. The same will happen with a message from an election official saying that all ballots from the voter should be cancelled. At the end of the election period, the election system will pick the last received ballot (if no cancelling message exists), remove the outer envelope by using the public key of the voter to check the signature on the data (the ballot) and, if verified, drop the inner envelope with the ballot in the electronic ballot box. From this point, there is no connection between the identity of the voters and the content of the ballots. The anonymous enveloped ballots will then be unsealed by decrypting the session key with the private key of the election event (which until then is kept secret inside a security module) and then decrypting the message with the session key.

---

[1] It is preferred that this key pair is used for much more than just electronic voting – the best solution is that the key pair is a part of an officially recognised PKI-system. This will reduce the possibilities for that the voter is selling the key pair.

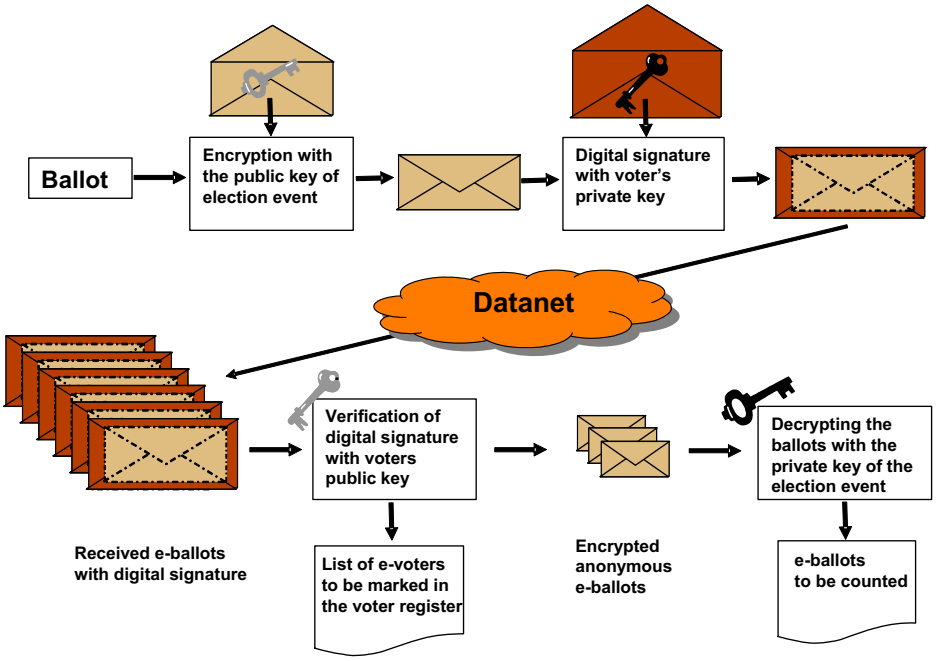

Figure 1: The double envelope principle

3.2 Letting the voter check the ballot

Returning to the question of how to convince the voter that his vote has been properly received, we propose that the doubly encrypted vote is returned to the voter client from the vote-storing server. In this case, the vote-storing server should sign it so that the user is convinced that the vote-storing server is actually storing the ballot. We also propose that the voter at any time during phase one of the election event may request the vote-storing server to send the doubly encrypted ballot to his client.

To be able to decrypt his ballot, the voter must have stored the session key used during voting somewhere. He may have written it down (not very likely), or stored it on a removable storage unit like a memory stick. To store it on the hard disk of the voting client is not to be recommended, for obvious security reasons. With the session key, it is possible for the client machine to open the two envelopes and show the voter the content of his ballot. The outer envelope is opened by decrypting with the public key of the voter, the inner envelope is opened by decrypting with the session key (we are of course not interested in the encrypted session key). The sceptical voter may do this on a client machine different from the one he used for voting – the likelihood that some evildoer may have managed to infect both machines with malicious software that even must show a consistent behaviour, is very small. In the future, this decrypting process may even be done by a mobile phone, so that the voter can use different technical channels for voting and for checking the ballot.

It may well be argued that this functionality is in conflict with paragraph 51 of the Recommendation [Rec2004], stating that ”A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.” If the voter, for any reason, wants to do it, he may show the content of his ballot to anybody, print it or e-mail it, just as he wish. The answer to this objection is of course that the voter may choose to cast another (and maybe completely different) vote at a later stage. Hence, seeing a copy of a ballot stored on the vote-storing server says next to nothing about how the voter finally is going to vote.

The second part of building the voters trust, namely that the final ballot will be dropped in the electronic ballot box, kept anonymous and properly counted, must be solved in a completely different way. The solution here is to use carefully designed and programmed software; verified and certified by an accredited certification institution. Additionally, if deemed necessary, the whole process may be run in parallel on different machines with different software developed by different developers with different methods, and compare the results – so called N-version systems [Liburd2004]. This is possible because this part of the election process can be run on a very limited number of machines in a heavily controlled and secured environment.

3.3 Keeping the votes anonymous

The anonymity of the votes (the impossibility of connecting the content of the ballot to the identity of the voter) rests on the principle that the double enveloped ballots and the private key of the election event should never be available to any person at the same time. Since it is difficult to keep the distribution of the double envelopes stored on the vote-receiving server under complete control (they may be logged for security reasons, or perhaps even copied by a hacker misusing the available functionality for checking the ballot), the solution is to handle the private key of the election event very carefully. It should be stored in a security module (separate hardware container) until it is time to open the inner envelopes, and it should be disposed of as soon as this task is done. In this case, a pin code may also be required in order to enable use of the key.

The degree of anonymity possible with a traditional paper ballot system cannot be guaranteed by an electronic voting system, however, these and other technical means can be employed to guarantee anonymity as far as possible. A security audit is essential to be able to track whether or not the election event key is being misused at any time.

If this solution does not look trustworthy, additional security may be achieved by using voter pseudo-identities. This, however, complicates the task of getting hold of the public key of the voter when opening the outer envelope and the latter solution has therefore not been recommended by the working group.

4 An overall picture of the architecture

Figure 2 depicts the overall architecture of the voting system. In the complete report written by the working group [KRD2006], the functionality of each module is described by means of UML Use cases.

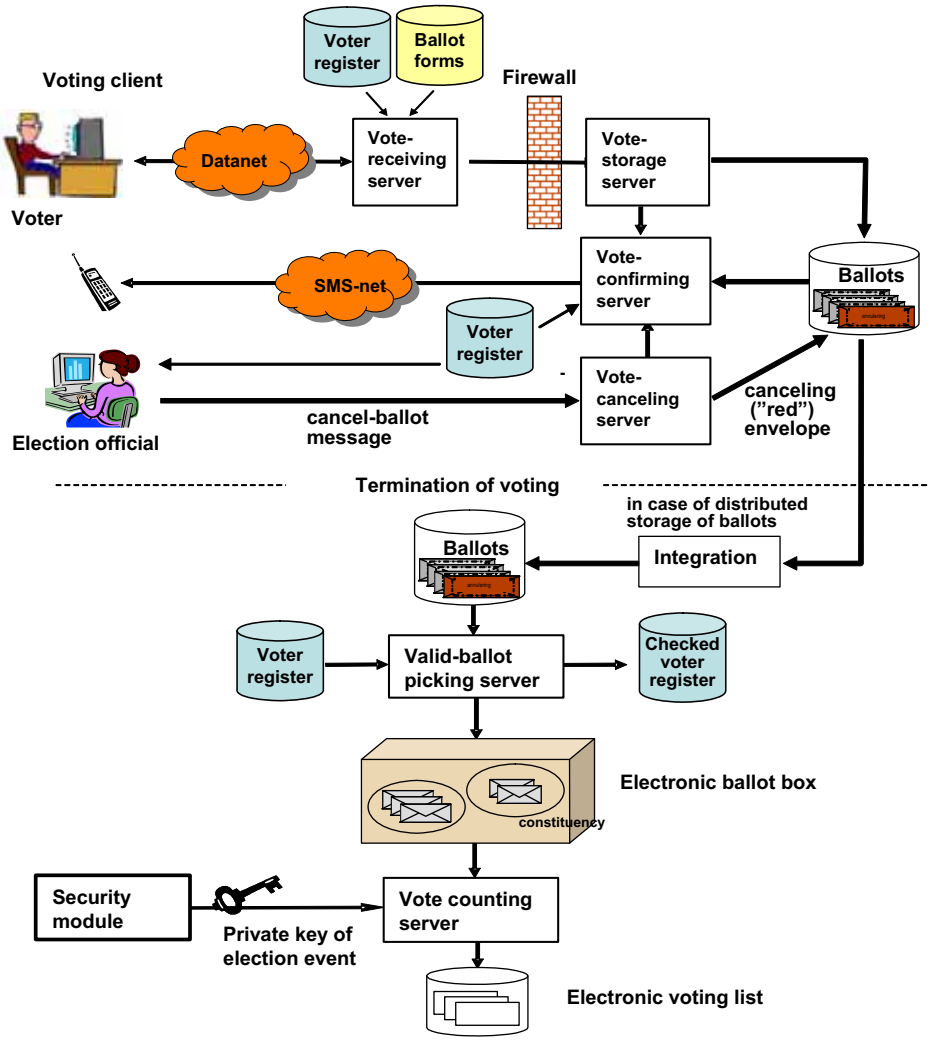

Figure 2: The architecture

5 Other security issues

Securing the availability of the vote-receiving server and other entities involved in the process is essential for the electronic voting to be conducted fairly. It is crucial to ensure that the vote-receiving server does not go down – in particular on the last day. Actually, last year the electronic tax return system in Norway failed to deliver on the last day [Ryv2005], and as a consequence, the deadline for submitting tax returns was extended by one day. For that service this was acceptable to the public, but would the citizens accept such a delay in e-voting? An issue related to this is protecting the vote-receiving server from so called denial of service (DoS) attacks aimed at making the vote-receiving server unavailable. Therefore we envision that a complete election system will encompass several vote-receiving servers, located in different geographical areas. On the other hand, we may have only one vote-storage server, but with well developed backup facilities.

The availability of the underlying network must be also be secured – attacks on parts of the network to take down network segments in order to prevent voters from being able to cast their votes should be anticipated. In a close election, targeting specific neighbourhoods that are known to favour the opposing side by e.g. flooding the local network to prevent votes from being cast electronically is easily carried out. This risk can be mitigated by the solution presented in this paper under the assumption that it is difficult to ascertain when voters will cast their votes. However, traffic analysis over several elections might reveal information on how likely it is that voters cast their votes ahead of time instead of waiting until the last day – one can predict that most people will wait until the last day to cast the final vote. In this case it should be expected that sabotage by creating denial of service attacks targeting the voting traffic may be widespread. Preventing this type of sabotage will be challenging, as known attacks may be easy to prevent, but new and effective attacks may come as a surprise, making it difficult to even mitigate the attack. We only have to look at the example of sabotage of the "Get out the vote" operations regarding organized phone jamming during the 2002 Senate race in New Hampshire in the United States [Coh2006] to get a flavour of how easy it may be to attack the underlying network. A very big concern with this type of sabotage carried out in a broadband network (both fixed and mobile) is that it may be difficult to discover, and the extent of the sabotage may not be uncovered until long after the election results have been certified.

This is only one example of electronic vote sabotage. For the system described in this paper, sabotaging the electronic vote system by attacking the underlying untrusted network should be considered carefully. For example, in a broadband IP-based network it may be easy to prevent users from voting electronically or prevent the ballots from arriving. This type of attack is of course easily discovered by the user, but if the user does not anticipate that this may be a problem and waits to the last minute to cast his/her vote electronically, he may be forced to go the polling place the over next day.

The attack scenarios discussed here show that it is difficult to ensure that voters will have completely equal access to the electronic voting system.

6 Conclusions

We are of the opinion that an e-voting system based on the principles described in this paper has the potential of being universally trusted by the voters, the election administrators, the politicians and the society in general. The principle of repeated vote-casting alleviates the well known democratic concerns with electronic voting in uncontrolled environments. At the same time, it allows for the voter to inspect his ballot as it is stored on the vote-receiving server without threatening the secrecy of the final and counting vote. In order to make it possible for the voter to decrypt the doubly enveloped ballot, the session key used during vote casting must have been stored on some medium, for example a memory stick. In order to build trust to the part of the system which is picking the valid votes and counting them, this part of the system should be designed and programmed very carefully, and verified and certified by an accredited certification institution. If deemed necessary, the whole process may be run in parallel on different platforms and the results compared (N-version system). However, it will still be difficult to ensure that voters will have completely equal access to the e-voting system.

References

[Coh2006] Cohen, A.: *A small time crime with hints of big time connections lights up the net*. http://www.nytimes.com/2006/04/17/opinion/17mon4.html?_r=3&oref=login&pagewanted=print&oref=slogin

[KRD2006] Rapport: Elektronisk stemmegivning – utfordringer og muligheter. Kommunal og regionaldepartementet 2006. (In Norwegian – an English version will follow.) http://odin.dep.no/krd/norsk/dok/andre_dok/rapporter/016051-220022/dok-bn.html

[Liburd2004] Liburd, Soyini: *An N-version Electronic Voting System.* Caltech/MIT Voting Technology Project Working paper # 17, July 2004 http://vote.caltech.edu/media/documents/wps/vtp_wp17.pdf

[Maaten2004] Maaten, Epp: *Towards remote e-voting: Estonian case*. In Prosser & Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society. Proceedings, Gesellschaft für Informatic 2004. http://www.e-voting.cc/files/E-Voting-in-Europe-Proceedings/

[NEC2004] The National Election Committee: *E-Voting System – Overview* http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

[Rec2004] Recommendation No. R (2004) 11 of the Committee of Ministers to member states on E-voting

[Ryv2005] Ryvarden, E.: *Skatte-servere tålte ikke trykket*. Digi.no, April 30 (2005) (in Norwegian)

[THJ2004] Johannessen, Tor Hjalmar: *On the mobile, its security issues and applicability potentials.* Teletronikk, 100 (1), ISSN 0085-7130, 2004.

Session 5: Redesigning Workflows for Electronic Voting

A generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process

Alexandros Xenakis, Ann Macintosh

International Teledemocracy Centre
Napier University, Edinburgh
{a.xenakis | a.macintosh}@napier.ac.uk

Abstract: In this paper we suggest a generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process. Based on the hypothesis that the electoral process has been through a "silent" re-engineering phase, we present the process re-engineering concepts which can be used to depict the redesign of the electoral process to an e-electoral process through the use of ICTs. Following we provide a five stage outline of the suggested re-engineering methodology. Finally we discuss the benefits of its implementation and suggest areas for its prospective application.

1 Introduction

The purpose of this paper is to present the process re-engineering concepts which can be used to depict the redesign of the electoral process to an e-electoral process through the use of ICTs and more importantly suggest a generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process. The paper is based on a completed doctoral research founded on evidence deriving from the case of the 2002 and 2003 UK e-voting pilot schemes. Reflecting the UK government's intention to develop "the capacity of holding an e-enabled general election some time after 2006" [HG 02] (p.47), 16 local authority legally binding e-voting pilots took place on May 2002 followed by 20 more pilot schemes held during the local authority elections on May 2003. This research addressed the following overarching research question: *"What are the non-technical constraints in re-designing the electoral process in relation to ICTs?"*

The analysis of the e-electoral process conducted, was based on the hypothesis that the electoral process has been through a "silent" re-engineering phase. That had lead the authors to adopt a process stage approach for its analysis and suggest the use of process re-engineering methods to support its future deployment [XM 03a, 03b]. However, no evidence has been identified to suggest that any kind of organized re-engineering attempt of the traditional electoral process has been undertaken prior to the deployment of the UK e-voting pilots. According to the UK Government, future e-enabled electoral processes and services could be deployed in relation to [HG 02]:

1. Elections to the Westminster Parliament
2. Elections to the Scottish Parliament
3. Elections to the Devolved Assemblies (Wales and Northern Ireland)
4. Elections to Local Councils
5. The conduct of referendums
6. Private ballots under statutory control
7. The on-line registration of voters
8. The on-line application to be an absentee voter.

All the above electoral processes present many differences between them in terms of surrounding legislation, electoral system used, political importance, social background of the electorate and its resulting electoral behaviour.

2 The use of process re-engineering in government provided services

Electronic voting is an interdisciplinary field of research based on the collaboration of a number of well established scientific fields. Computing experts need to co-operate with sociologists, political scientists, and media communication experts. Moreover, e-voting research particularly requires the contribution of legal and public administration experts. E-elections, similar to traditional elections, are government owned and initiated processes, and as such, many of the activities involved in their undertaking are closely related to public administration, in this case electoral administration in particular. In the past, process re-engineering in the public administration sector has been widely used to re-organise other administrative processes that had to be redesigned due to the introduction of ICT in some or all of their stages. Thaens [TBD 97] has discussed the use of BPR (business process re-engineering) in the case of taxation. Bellamy and Taylor [BT 97] have referred to the use of adaptive information systems in the case of the UK Criminal Justice System. Pollard [Po 97] has analysed the case of organisational transformation of the National Mapping Agency of Great Britain. Willcocks [WCJ 97] provides detailed analysis of three cases in the UK related to the healthcare sector and the postal service. Van Belle [VB 97] discusses the case of re-engineering the Flemish Department of Education with the purpose of introducing ICT. Lenk [Le 97] has explored the enabling role of ICT in relation to the risks and opportunities involved, stating the need for continuity of structures of accountability. Pratchett [Pa 97] focuses on the use of BPR at the local authority level, referring to the level of radical re-engineering, the suitability of processes to undergo re-engineering and the level of dependence on ICT. Zuurmond and Snellen [ZS 97], on the other hand, take a more managerial approach discussing organisational structures and informational architectures within the bureaucratic paradigm.

In this paper the authors suggest the development of a generic electoral re-engineering methodology. Such a methodology has the potential to support the structured re-engineering of any electoral process providing a fit for purpose approach based on the experience gained to this date.

3 Research methodology

Initially, BPR concepts are used to assess the redesign of the electoral process to an e-electoral process and analyse the resulting effects on the validity of the process, the effectiveness of its administration and the social acceptance of its results. In the past, process re-engineering in the public administration sector has been widely used to re-organise other administrative processes that had to be redesigned due to the introduction of ICT in some or all of their stages. However, it was necessary to adapt the process re-engineering rational to the characteristics of the particular process analysed, which in this case is the electoral process. The challenge was to identify the different sub-processes (stages) that take place within an e-election and decide which process re-engineering concepts can be beneficially used in their analysis.

The purpose of the following section is to present the BPR concepts used to depict the redesign of the electoral process to an e-electoral process through the use of ICTs and analyse its resulting effects. To that effect a review of existing BPR methodologies was conducted in order to identify the key BPR concepts which can support the analysis of the e-electoral process. The theoretical BPR concepts presented hereafter form the basis of the process stage approach to the e-electoral process adopted in this paper. The main BPR concepts used are:

- Agent roles and their procedural responsibilities
- Agent accountability and agent obligations
- The definition of agent dependencies
- Multiple agent communication, co-ordination and control

All of the above concepts have been useful for the analysis of the three non-technical aspects of e-voting explored during this doctoral research. Defining, and re-defining agent responsibilities was used for the analysis of the trust relationships developed between agents to support the social acceptance of the e-electoral process. Defining agent accountabilities was used for the analysis of the procedural security aspect of e-voting. Finally defining dependencies and exploring how multiple agent communication, co-ordination and control mechanisms can be applied in the deployment of e-voting was useful for the analysis of the e-electoral administration.

4 Essential BPR concepts used for the analysis of the e-electoral process

This section provides a reference to the essential BPR concepts which can support the analysis of the e-electoral process.

- Defining agent roles and their procedural responsibilities

Roles are related to agents who operate under an obligation to fulfil certain responsibilities. Simple actions are assigned to agents through roles. Processes are composed from the combination of these simple actions. Roles define an agent's state at any point in time. Agents rationally choose their next action according to the options associated with each specific role [Hi 85]. The description of e-voting agent roles can serve the detailed allocation of tasks attributed to each agent. This aspect mainly aims at the allocation of procedural responsibilities but also enables a better understanding of the overall process.

- Defining agent accountability and agent obligations

The notion of agent accountability is closely related to the identification of responsibilities. A person is held accountable by others in relation to the fulfilment of one's responsibilities, which will in turn create procedures even if not originally defined [Sc 93]. By identifying agent responsibilities one can also identify their procedural obligations. Obligations limit the choice of action, and therefore need to be fulfilled according to the undertaken responsibilities. Responsibility is 'for' something; obligation is 'to do' something. Obligations are concerned with keeping things the way they are or changing them in relation to the responsibility held [DM 89]. The satisfaction of obligations is achieved by the introduction of rules which constrain agents' actions. Rules are therefore constraints put on people by the organization on how they should act [Ou 92]. Constraints are thereafter inherited by processes and activities either partially or in full. In the e-voting context, business rules are substituted by the existing legal framework defining an election, as legislation varies according to different elections. We should therefore consider the relevant legal issues as a dynamic factor to which e-voting deployment should adjust accordingly.

- Defining dependencies

When agents participate in contractual relationships, they undertake a set of responsibilities that are determined by the terms of any given contract. Within an organization, contractual (responsibility) relationships determine the type of the structural relationships between pairs of co-workers whereas, a contractual relationship between an external agent and an organization exists only for the duration of a specific contract. The notion of contractual relationships is broadly used by the UK civil service where independent agencies provide the central government with their services therefore developing a contract between them [HT 88]. The analysis of contracts will in turn help identify agent responsibilities and dependencies among them, deriving from their participation in contractual relationships. Once agent responsibilities have been identified they can subsequently be allocated along the e-voting process. Defining dependency relationships between the different collaborating parties in the e-voting procedures can be achieved by clearly demonstrating each agent's role and internal responsibilities. The focus should be on the identification of dependencies that are critical for the election success.

- Enabling multiple agent communication, co-ordination and control
According to Mintzberg [Mi 89] there are six types of coordination mechanisms:

1. Mutual Adjustment (informal communication)
2. Direct Supervision (common supervision of people whose work is related)
3. Standardization of the work processes (when different tasks involve different people in one process)
4. Standardization of outputs (specification of expected results)
5. Standardization of skills (based on the training of the people involved in the process)
6. Standardization of norms (describing a process so that everyone involved has the same understanding of it)

The co-ordination of the agents involved in the delivery of electronic voting is of central importance due to their multiplicity and the complex nature of the multiple channel e-voting process.

5 A five stage approach to electoral process re-engineering

The following sections provide a five stage outline of the suggested generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process.

5.1 Understanding the context of the existing electoral arrangements and the aspirations of the main government organisations concerned

The first stage of e-electoral redesign is a diagnostic one. The aim is to have a full understanding of the electoral process which is going to be re-designed to an e-electoral process. Initially, one has to identify the government agents involved in the voting procedures. Related government agents should be approached for data which will be later used for both modelling and analysis of the process. The primary aim is to gather internal data, in any form (previous e-voting evaluation reports, statistics, cost calculations etc.). Organizational data could also be collected from a variety of internal sources.

That should be followed by interviewing representatives of these agents. When conducting interviews with the government organisations' departmental managers, one should try to identify opportunities for improvements and understand the organisations' culture. These interviews will also identify further data collection opportunities and determine the focus issues which will constrain the re-design of the process. Interviews should however be focused on identifying:

- Each related department's tasks, responsibilities and activities in relation to the electoral process
- Expected inputs and resulting outputs related to the above activities

- Input suppliers and output customers for these activities, whether internal or external
- Formal and informal communication lines

After concluding the above practices a decision has to be taken by the main government organization concerned as to whether re-engineering will be aiming at process improvement (an e-enabled paper ballot based election) or process innovation (an e-voting process possibly including an e-enabled element as well). This would derive from the combination of the opportunities identified in the earlier steps and the aspirations of the government organisation, meaning the amount of risk they are willing to take.

In the final part of this stage, once the data has been gathered and evaluated and the decision on the aim of the re-engineering has been taken, a document should be prepared containing the specific objectives of the re-engineering effort.

5.2 Modelling (who, what, where and how)

The modelling of the existing and proposed electoral process will be based on the information gathered in the previous stage. The primary concern when modelling the processes is to:

- Further analyse the agents involved into macro agents and micro agents. According to [Jo 89] micro agents are individual persons whereas macro agents are entities like organizations and companies. Macro agents have micro agents as parts.
- The identification of agent roles and resulting responsibilities
- Identification of critical contractual relationships between agents involved in technology provision contracts, authority contracts in bureaucracies (administration contracts) and long term unwritten contracts within groups based on principles of mutual latent trust.
- The identification of objectives, interactions and dependencies resulting from the above contracts
- The fragmentation of processes into stages including smaller operation and activities
- The identification of coordination and control mechanisms
- The explicit identification and statement of rules (whether legal or otherwise) limiting all the above

Three basic model constructs are suggested:

- Process stage modelling (what needs to be done and when)
  By modelling each stage of the electoral process, one can monitor the parallel activities taking place concurrently. Such models can be used to describe the activities taking place (what needs to be done) in the different stages of the e-electoral process (and when). Representing agents within the process stage models would extend their descriptive functionality.

- Contractual relationships modelling (who should deliver what and who expects what)
  The contractual relationships perspective could be modelled so as to identify the obligations of each agent towards others (who should deliver what) and accordingly the deriving dependencies of deliverables between agents (who expects what)

- Agent role modelling (how should agents act)
  The focus of these models should be on roles, activities and the agent responsibilities deriving from those activities. The question here is to define how the agents identified should respond to their responsibilities (how should agents act) within their combined activities which produce the overall electoral process.

5.3 Analysis (why)

The purpose of the analysis of gathered data, existing and proposed models, is to understand why process stages, contractual relationships and agent roles are executed in the way identified. Analysis tools and methods can either be developed or alternatively **adapted as appropriate from those having already been used in the re-engineering of** business processes. A set of analysis methods which have been used in BPR and could potentially prove useful for the analysis of the e-electoral process include:

- Analysis of the abstraction level of the prepared models, testing for clarity and transparency [IH 92].
- Principal-Agent analysis of the contractual relationships related to agent co-ordination, management and control [FJ 83]
- Management structure analysis to evaluate the use of management resources, by looking at issues such as span of control and layers of management [BC 91].
- Mission/non- mission analysis to assess whether an agent's obligations are critical to the achievement of the process objectives [Gl 94].
- Fragmentation-concentration analysis to define the number of full time equivalent employees needed to undertake an activity, in this case related to the issue of costs and the number of staff needed for the deployment of e-voting [Ha 90], [DS 90].
- Fractionalisation analysis to establish the level of fragmentation of an employees work and consider whether the responsibilities undertaken by each agent are correctly allocated to the agent in question according to time and expertise [Gl 94].

At the end of this stage one should have a full understanding of the current electoral arrangements, the proposed changes to the electoral process and the resulting effects that these changes would incur in terms of security, administration and social acceptance of the e-electoral process.

5.4 Re-design

In this stage the conclusions reached in the analysis undertaken in stage three, together with the proposed would-be models, and the models of existing electoral arrangements produced in stage two should be presented to the main government agent holding the election. A second round of interviews, this time including more junior employees could identify further opportunities for improvement and validate those already identified. Employees should be asked to contribute to the validation of the would-be models before those are applied so as to finalize them.

The internally gathered data could be supplemented by external data about known best practice on the deployment of e-voting. However this should be relevant to the specific objectives of each re-engineering exercise. If for example the aim is to introduce a certain type of e-voting technology then one should look into past experience using the same kind of technology. Nevertheless, e-voting is still at a pilot stage and accumulated best practice is hard to identify for two main reasons. Firstly there is little experience in large scale e-voting deployments. Secondly, in order to define best practice one has to set commonly accepted evaluation criteria, or at least accepted in the context of a specific re-design effort. Widely recognized best practice will take a certain amount of time and testing to develop in the e-voting environment.

The outcome of this stage should be a re-designed e-electoral process, the re-design solutions being based on the organised introduction of ICT in the traditional electoral process.

5. 5 Continuity of e-electoral redesign

This last stage should be concerned with maintaining the benefits gained during the re-design effort. The necessity for adaptation to e-voting technology advances, as well as to changing voter trends, fosters the necessity for repetitive process improvement. Continuous staff training should also be undertaken, responding to the need for additional technical, procedural and managerial skills. This doctoral research produced three separate analytical methods for the evaluation of e-electoral processes which could serve the continuous assessment of e-voting schemes:

- Procedural security analysis [XM 04a], in which given security constraints are used as evaluation criteria to measure the existing or prospective security level of e-electoral procedural practices
- Trust flow analysis [XM 04b], a method which provides an abstract representation of how stakeholders interact in terms of trust within the scope of a re-designed electoral process
- Level of difficulty analysis [XM 04c], which evaluates the expected level of difficulty of a suggested e-voting scheme prior to each implementation based on specific criteria.

6 Conclusions

Defining roles and responsibilities within the e-voting process could provide a better understanding of who is responsible for doing what in the different process stages so that the election result is produced. Transparency of operations could provide a better insight of agent interactivities. Thus, the comparative analysis of agent roles between the traditional and the new e-electoral process could be used to specify how agent responsibilities and obligations are altered and re-distributed due to the introduction of ICTs in the electoral process. This in turn supports trust analysis and social acceptance [XM 05].

Procedural risks such as user errors could be identified in the analysis of the e-voting process and therefore either predicted or counter-measured in a way that the outcome of the process would not be endangered. The identification of procedural security gaps which could foster fraud opportunities and their allocation to specific process stages could function as a preventive mechanism against the possibility of fraud in all its different forms. Hence this line of research would support preventive management of e-voting fraud.

Better management could be provided by identifying the opportunities for effective administration of the introduced e-voting technologies. This is in line with the requirement for customisation of e-voting technology to fit local needs and the need for common evaluation criteria on the effectiveness of e-voting technology. The stage analysis of the e-voting process could also prove beneficial in the effective allocation of resources by indicating the optimal combinations of resources in parallel process stages of the multiple channel e-voting process. Finally, the re-engineering of the process could lead to process simplification, which is also a necessity in the deployment of e-voting.

7 Future work: Investigating cost efficiencies for e-voting

The matter of cost is considered to be a defining factor in the deployment of e-voting in all major e-voting reports related to the UK context [Co 02], [Pa 02], [FR 02]. Government organisations need to manage the economic risk of investing in e-voting technology and make a return on their investment. According to the Electoral Commission one of the main reasons for piloting e-voting was to establish whether cost efficiencies can be achieved. Although a lack of a specific methodology to measure and evaluate the cost of all the different e-voting channels and their combinations is formally acknowledged, the Commission does consider paper ballot e-counting as having established its related cost efficiencies, hence the limited number of e-counting pilots in the 2003 pilot schemes [Ec 03]. A further issue is the documentation of the experience gained in this area. Although detailed evaluation reports have been produced with regard to technical, security, legal and accessibility issues, to this date no detailed study has been published with regard to e-voting costs.

The deployment of electronic voting systems requires considerable initial investment, operation and maintenance costs. Alternative combinations of e-voting or e-enabling technologies can result in different financial requirements. The authors therefore suggest that future research is oriented towards producing a cost accounting methodology aiming at estimating and controlling multiple channel electronic voting costs. There is an apparent need to define specific cost metrics so that when one refers to the costs of e-voting there is mutual understanding. Such research would answer e-voting costs criticism which is fostered by the absence of specific cost metrics. The authors also suggest that any cost methodology should not cover e-voting channels alone, but the combination of e-channels with paper-based channels (postal and polling station voting). If a process stage approach is adopted for all the different channels, then common costs can be identified and economies of scale can be calculated for different combinations of multiple channel elections. Possible cost reductions could be identified by allocating costs between the different stages, agents and objects involved in the process. The modelling of the e-voting process could also prove beneficial for the optimum allocation of resources, by representing the alternative options of allocating resources between the parallel stages of different voting channels. Future pilot projects offer an excellent opportunity for such a study according to the scale and the nature of the pilot, providing that precise cost estimates and final costs are kept during the pre-electoral period in a concise, pre-defined format.

The cost deriving from the adoption of e-voting systems and whether this can be considered as justifiable is a matter of policy. In one of the interviews held during the fieldwork of this doctoral research with the Returning Officer of the UK local authority where observations of an e-voting scheme were undertaken, the RO expressed the following opinion on the matter of cost:

*"In the issue of setting this (*e-voting adoption*) in priority to other priorities, when you've got basic services that need to be delivered, it means that members (*local councillors*) will have to take a very long hard view"* adding that *"if they have to make a choice between whether they spend money on the voting structure as opposed to spending money on street lights then it becomes a very difficult choice"*

E-voting costs nevertheless should be measured against the expected added value that their deployment will incur in the wider democratic process. Usually, the prospective benefits from the introduction of e-voting technologies are related to the hypothesis that the convenience offered can be used as a counterbalance against voter apathy and therefore increase voter turnout, which in turn legitimises the outcome of the electoral process. A further hypothesis is based on the assumption that young voters who are familiarised to the use of technology in general, are more inclined to participate in the electoral process if presented with the opportunity to use technological means to cast a ballot. However both of the above assumptions remain to be proven. Eventually, if no apparent relationship between e-voting and increased voter turnout is achieved, then the future of e-voting will lay solely upon the cost factor as far as the state is concerned and the trust factor from the voters' point of view.

References

[BT97] Bellamy, C. & Taylor J.A. (1997). Transformation by Stealth: the case of the UK Criminal Justice System. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 37-54, IOS Press.

[BC91] Butler-Cox Foundation (1991). The Role of Information Technology in Transforming the Business: Management Summary, Report 79, January 1991.

[Co02] Coleman, S. & Independent Commission on Alternative Voting Methods (2002). Elections on the 21st Century: from paper ballot to e-voting. Electoral Reform Society.

[DS90] Davenport, T.H. & Short, J.E. (1990). The new industrial engineering: Information technology and Business Process Redesign. *Sloan Management Review* vol.11.

[DM89] Dobson, J.E. & McDermid, J.A. (1989). Security models and enterprise models. In Landwehr, C.E. (ed*.) Database Security: Status and Prospects II*, Amsterdam: Elsevier Science.

[Ec03] Electoral Commission (2003). The shape of elections to come: A strategic evaluation of the 2003 electoral pilot schemes, July 2003

[FR02] Fairweather, B. & Rogerson, S. (2002.) Technical Options Report, De Montfort University, Leicester.

[FJ83] Fama, E.F. & Jensen, M.C. (1983). Separation of Ownership and Control*. Journal of Law and Economics* vol.26, pp.301-326.

[Gl94] Glykas, M. (1994). "Agent Relationship Morphism Analysis" PhD thesis, University of Cambridge.

[Ha90] Hammer, M. (1990). Re-engineering work: Don't automate, Obliterate. *Harvard BusinessReview,* July-August 1990.

[Hi85] Hirscheim, R.A. (1985). *Office Automation: A Social and Organizational Perspective*. Chichester: Wiley Series in Information Systems.

[HT88] H.M Treasury (1988). Improving management in Government: The next steps. Efficiency Unit, HMSO.

[HG02] HM Government (2002). In the service of democracy, a consultation paper on a policy for electronic democracy.

[IH92] Ip, S, & Holden, T. (1992). A Knowledge based technique for the process modelling of information systems: The Object Lifecycle Diagram. *In proceedings of the 4th conference of Advanced Information Systems Engineering*. Manchester, UK.

[Jo89] Johansson, I. (1989). *Ontological Investigations: An Inquiry into the Categories of Nature, Man and Society*. London: Routledge.

[Le97] Lenk, K. (1997). Business process reengineering in the public sector: opportunities and risks. In Taylor, J.A., Snellen I.Th.M. and Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 151-165, IOS Press.

[Mi89] Mintzberg, H. (1989). *Mintzberg on Management.*. New York: The Free Press.

[Ou92] Ould, M.A. (1992). Process modelling with RADS*. IOPener* 1(5).

[Pa97] Pratchett, L. (1997). Reengineering UK local government: opportunities and prospects. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 165-188, IOS Press.

[Pa02] Pratchett, L. (2002). The implementation of electronic voting in the UK. LGA Publications, The Local Government Association.

[Po97] Pollard, P. (1997). Organisational Transformation and the commodification of spatial data: a case study of the National Mapping Agency of Great Britain. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 71-89, IOS Press.

[Sc93] Scheer, A.L. (1993). A new approach to business processes. *IBM Systems Journal* 32(1).

[TBD97] Thaens, M., Bekkers, V.J.J.M., van Duivenboden, H.P.M. (1997). Business Process Redesign and Public Administration: a perfect match ? In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 15-36, IOS Press.

[VB97] Van Belle, J.L. (1997). Reengineering administration: the case of the Flemish department of Education. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 133-149, IOS Press.

[WCJ 97] Willcocks, L.P., Currie, W.L., Jackson, S. (1997). In Pursuit of the re-engineering agenda: research evidence from the UK public services. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 103-132, IOS Press.

[XM03a] Xenakis, A. and Macintosh, A. (2003a). Using Business Process Re-engineering (BPR) methods and analysis tools to effectively implement electronic voting. *Proceedings of the 3rd European Conference on E-Government ECEG 2003*, Ireland.

[XM03b] Xenakis, A. and Macintosh, A. (2003b). A Taxonomy of Legal Accountabilities in the UK E-voting Pilots. *Proceedings of EGOV 2003, the 2nd International Conference on Electronic Government*, Czech Republic.

[XM04a] Xenakis, A. and Macintosh, A. (2004a). Procedural Security Analysis of Electronic Voting. *Proceedings of ICEC 2004*, *6th International Conference on Electronic Commerce* Netherlands.

[XM 04b] Xenakis, A. and Macintosh, A. (2004b). Trust in public administration e-transactions: e-voting in the UK. *Proceedings of TrustBus 2004*, *1st International Conference on Trust and Privacy in Digital Business,* Spain.

[XM 04c] Xenakis, A. and Macintosh, A. (2004c). Levels of difficulty in introducing e-voting. *Proceedings of EGOV 2004, the 3rd International Conference on Electronic Government,* Spain.

[XM 05] Xenakis, A. and Macintosh, A. (2005). Procedural Security and Social Acceptance in E-voting. *Proceedings of HICSS-38 Thirty-Eighth Annual Hawaii International Conference on System Sciences*, USA.

[ZS97] Zuurmond, A. & Snellen I.Th.M. (1997). From Bureaucracy to infocracy: towards management through information architecture. In Taylor, J.A., Snellen I.Th.M. & Zuurmond, A. (eds). *Beyond BPR in Public Administration: an institutional transformation in an information age,* pp. 205-224, IOS Press.

Election Workflow Automation - Canadian Experiences

Goran Obradovic, James Hoover, Nick Ikonomakis, John Poulos

Dominion Voting Systems Corporation
20 Mowat Avenue
M6K 3E8, Toronto, Canada
{goran.obradovic | james.hoover | n.ikonomakis | john.poulos}@dominionvoting.com

Abstract: Democratic parliamentary and presidential voting supported by election systems worldwide represents the essential idea behind any free society. In recent years, numerous challenges have been overcome to satisfy this fundamental principle. On one side we have low voter turnout and high electors migration, on the other, sometimes complex electoral systems such as preferential or transferable ballot voting. In addition, proliferation of modern computerized technologies is giving hope that with new automated processes and voting channels, the election process and democracy as a whole can be more accessible, secure and transparent. In this paper we are presenting the Democracy Suite as the field-proven solutions for full election automation workflow.

1 Introduction

Governments in Canada are organized in a range of geographical structures. The federal government uses a single member plurality system in 308 ridings, also known as electoral districts. Similar systems are used in each province but with lower numbers of ridings. Municipalities use more complex structures – typically electing a single mayor and multiple councilors or trustees using composite ballots with several plurality contests. To date, preferential or transferable ballots have not been widely used but successful pilot projects are contributing to serious consideration. Elections dates in Canada can be divided into two general categories – fixed and variable. Most municipal events are on fixed dates and several hundred towns and cities can have elections on the same day. In contrast, provincial and federal governments are modeled on a parliamentary system so governments can be defeated at any time during a 5-year term.

In Canada, paper ballots and in-person voting are predominantly used for all types of elections. In some cases vote-by-mail is used as well, but in essence this voting channel still uses paper ballots with central vote counting. For decades, the voting process was mostly performed manually – electors were recorded using a hard-copy voters list and ballots were tabulated by hand. This basic system was acceptable for simple elections, but recording inefficiencies cause long line-ups at voter registration and manual vote tabulation leads to inconsistencies and long delays in results reporting.

Automation of vote tabulation has started in mid 1990's and was predominantly used for decentralized and centralized paper ballot processing for local elections in large cities. These first generation systems from Diebold and ES&S, designed before introduction of Voting Systems Standards [FEC02] and HAVA standards [HAVA02], didn't provide accessible, secure and transparent election process as required by [EA05]. In addition, lack of integrated elector management system, standard-based data interchange schemas and alternative remote voting channels, made those systems inappropriate for Canadian elections. Since late 2002, Dominion has been developing an integrated and automated election system under the name of Democracy Suite. This set of software applications and hardware devices, coupled with variety of services, provides a complete set of solutions for traditional in-poll or remote paper-based voting, electronic remote voting (Internet), and elector management. In this paper we will provide a brief technical overview of the Democracy Suite as it was deployed in the variety of elections in the provinces of British Columbia, Alberta, Ontario, Quebec and Newfoundland.

2 Automated Election Workflow

The overall election process schedule is separated into *election event* and *election cycle* activities (Figure 1). Election events represent specific voting occurrences, with its date and the jurisdiction of the given electoral authority, plus a unique set of *election entities*, such as polling divisions, contests, candidates, ballot styles, voting channels, etc. The election cycle activities, on the other hand, include elector management activities for obtaining the complete and most up to date list of eligible voters.

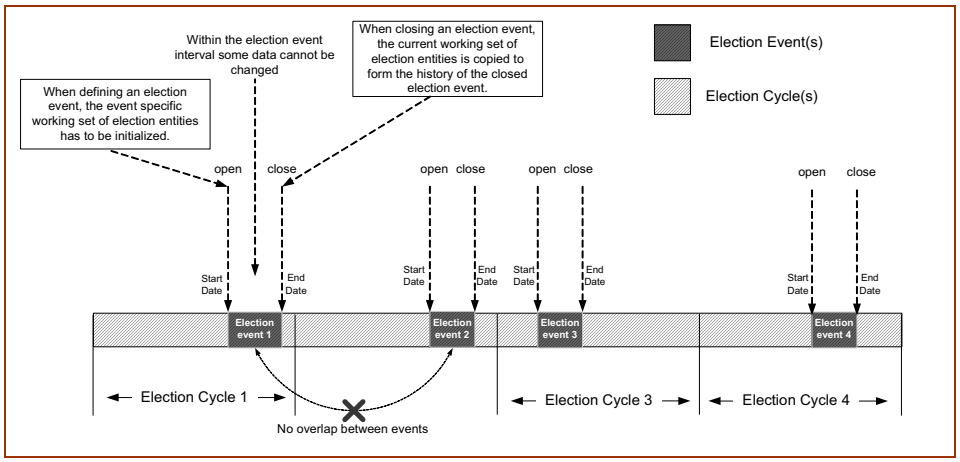

Figure 1: Relation between election events and election cycles.

Every election event begins by collection of election entity data. This election event definition phase primarily involves accumulation of contest and candidate names as well as all additional geographical and administrative information needed (polls, polling districts, polling locations, polling stations, etc.).

This data usually comes directly from electoral authorities responsible for event organization and enters our system in an XML defined schema for election entity information exchange, similar to EML [EML05]. After importing this data into our election event data model, the system proceeds with automated creation of ballot styles, voting information files needed for programming of voting channel devices, and election results reporting XML schemas.

All voting channels utilize a common set of configuration files (channel configuration and voting information files) which contain directives for the system operational and election rules (Figure 2). For data protection and performance issues, these files are encrypted and in binary format. Using this approach, complete and seamless integration of all system components is achieved - unifying diverse entities with clear technical separations (i.e. paper versus electronic ballots). Simply stated, the system provides a) only one point of definition for all relevant election data and b) only one point of tabulation from different voting channels. Figure 2 also shows different voting channels supported by our automated election workflow:

a) Decentralized poll-based voting using paper ballots and polling station tabulators (CF200 series)
b) Centralized voting using paper ballots and central count tabulators (CF500 Series)
c) Electronic remote voting using electronic ballots and Internet (e-Voting)
d) Fax-back remote voting using paper ballots and fax services
e) Vote-by-mail remote voting using paper ballots and regular postal services

Ballots cast, using any of the voting channels, are collected using the same central platform which performs a variety of tasks such as vote tallying, verification, auditing and publishing.

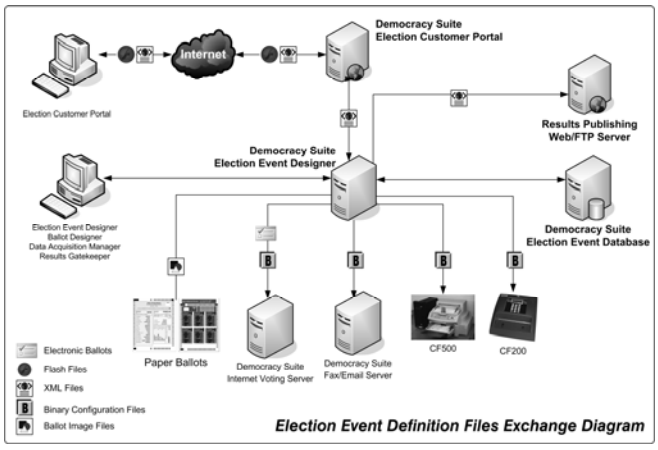

Figure 2: Election event definition files exchange diagram.

In addition, for full support of a variety of voting channels, Democracy Suite includes elector management support for registration and tracking of electors. This support includes day-to-day elector management (add, modify, delete), address management, and

administrative areas management tasks. For real-time voter tracking during election events, Democracy Suite creates an electronic poll-book list of electors which is synchronized with central elector register using GPRS/EDGE or regular Internet connectivity. Finally, the system provides full support for remote voting registration, such as vote-by-mail and Internet voting. Figure 3 presents an elector management deployment scenario.

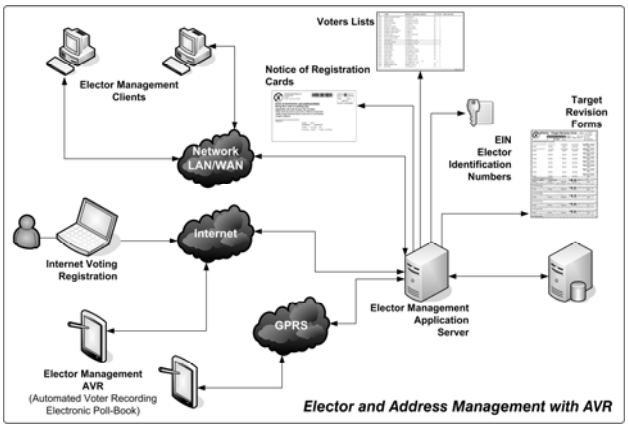

Figure 3: Elector and address management.

3 Data Model

The data model for our automated election services is structured around three databases: *elector management*, *election event*, *security* database. Each of the databases model the real election related entities and their relationships. Electors and their addresses, as well as related administrative data are stored in *elector management* database, together with the voting channel type and elector status (voted, not-voted). The *election event* database contains data related to particular election event such as contests and candidates. This database also stores voting results for a given election event. Finally, the *security* database models electoral organization roles, permissions and retains a log of all activities performed by the users of the system.

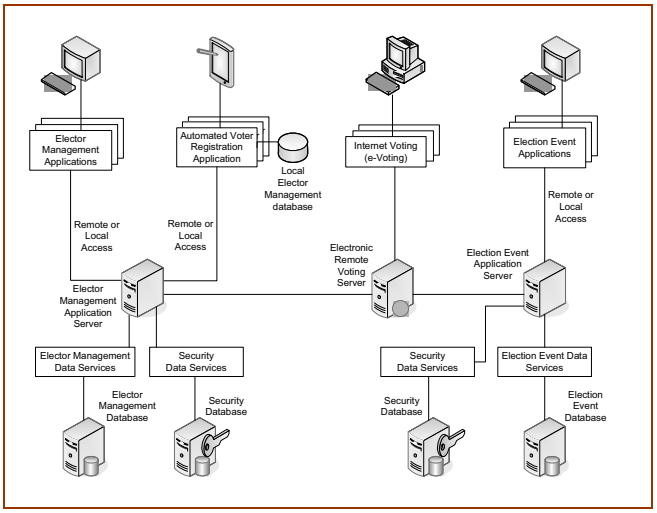

Figure 4: Data model for our automated election services.

The data in the Elector Management database model can be classified into the following categories in relation to an election event and election cycle:

a) Logically detached from election event
b) Logically attached to election event
c) Logically semi-detached from election event

The data in Election Event database has validity only during a particular election event for which they are defined – i.e. list of contest and candidates will change between different election events.

All the tables in our data models can be divided into four categories: *Entity*, *Type*, *Log* and *Mapping* tables. Examples of Entity tables are *Person*, *Poll*, *Candidate*, etc. These tables always use GUIDs as primary keys and contain primary election entities. Examples of Type tables are *LocationType*, *VotingChannelType*, etc. These tables always use integers as primary keys and define election entity or action types as enumeration values expressed in different languages. Examples of Log tables are *VotingLog*, *AdvancedVotingLog*, etc. These tables record all election cycle and election event related activities such as time and place where someone has been voting. Finally, Mapping tables provide support for various levels of relationships between different entities. Examples of these tables are *LocationHandlesPoll*, or *PollUsesBallot*, etc.

From software architecture point of view, both Election Event and Elector Management Application Servers, as guardians of database access and management, implement optimized and concurrency safe data access layers. These software components are not only responsible for direct database access, but also for Object to Relational Mapping (ORM) between database tables and their relationship on one side, and domain objects on the other. This architecture provides robust election specific domain access and clear view toward the election data models.

4 Democracy Suite Software Components

The two core software components of Democracy Suite are Election Event and Elector Management application server. These two server components implement automated election workflow intelligence and communicate with corresponding data models. These application server modules are deployed utilizing encrypted binary transport channels and a variety of client applications and dedicated task-oriented services:

a) Election Event Definition – set of pre-voting modules for defining election events, programming of the voting channels and creation of ballots, either paper of electronic.
b) Results Tally and Reporting – set of post-voting modules for acquisition of election results from the voting channels, manual data entry, results verification, tally and publishing. In addition, auditing of the overall voting process is integrated in this module.
c) Elector Management – responsible for the importing, cleansing, maintenance and real-time tracking and registration of electors. In addition to importing elector data from a variety of data sources, this system creates:
    i. Notice of Registration Cards (NRCs), or invitation to participate (vote) in a given election event.
    ii. Electronic and paper poll-book lists that can be used in combination with the our Automated Voter Recording system and the CF105 electronic poll-book platform,
    iii. Elector Identification Numbers (EINs) used as secure PINs for remote electronic voting (e-Voting), and
    iv. A list of voters and addresses for a subsequent target revision process which should provide a clean and up to date list of electors for the next election event.
d) Remote Electronic Voting – includes a support for Internet voting, which basically includes Registration Server, Electronic Ballot Issuing Server, Internet Voting Server and Electronic Ballots. All these components work in harmony with Election Event and Elector Management subsystems.

5 Automation of Paper Ballot Voting

A majority of the elections in Canada, and also in other parts of the world, remain based on a paper ballot system and in-poll voting. We can expect that this traditional voting channel will be in use for some time as a result of cost, accessibility, and permanent audit record considerations. Therefore, one of the primary goals of our strategy was to automate that process as much as possible using a specialized set of software and hardware solutions.

From a hardware point of view, we have designed an electronic voting box (CF200) in the form of optical ballot tabulator (Figure 5) with integrated audio vote capabilities and variety of communication options.

This device, especially designed for decentralized deployments (for in-person voting), deploys a reliable two-sided high-resolution digital scanning mechanism with on-board advanced image processing algorithms for optical mark recognition. Every ballot scanned is saved and permanently imprinted with the results of the vote determination algorithm. This patented feature provides a fully auditable paper and electronic trail. Also supporting special requirements for people with disabilities, the CF200 deploys audio ballot feature for greater accessibility. Visually impaired and other people with disabilities can use this feature to cast their votes.

Figure 5: The CF200 electronic voting box in the form of optical poll-level tabulator.

For all central count applications reliable high-speed scanning hardware has been integrated with high-performance and accurate image processing algorithms. Depending on the scanning performance, ballot size and layout requirements, appropriate central count solutions from CF500 series can be selected. The CF500 is the most suited for high-turnout elections with scan rate of 6000 ballots per hour and ballot size of up to A3 format, while the CF520/40 models are designed for mid-turnout elections with scan rate of up to 2500 ballots per hour and ballot size of up to A4.

The image processing module within Democracy Suite leverages the binary nature of the scanned ballot images and provides high speed tabulation utilizing a two-dimensional signal correlation algorithm for tracking form landmarks. Prior to this approach, the optical tabulation platforms used a rudimentary bounding box technique together with a straightforward pixel counting method for detecting form answer fields. Although this technique was extremely fast, it was highly susceptible to printing inconsistencies, scanning noise and image skewing. Furthermore, the decision process for any given voting field (i.e. detection of mark or no mark for a given candidate) employed fixed rotation bounding boxes that did not accommodate for even minor image skews.

In order to speed up processing, the new algorithm uses an iterative search space which converges on the location of the desired ballot marking field by varying the search space extent and resolution until a specified threshold is reached. This use of pattern matching is superior to a simple bounding box technique because it is able to filter noise more effectively as well as account for some variations in skew as the most likely result is used in the analysis of voting boxes. The new technique has been able to successfully detect votes that have been inadvertently cut off during scanning, markers obscured by printing or scan head artefacts, as well as markers that have been tampered with (e.g. written on). In addition, form skew is taken into consideration, allowing the bounding box of the answer area to be rotated appropriately, and thus provide more accurate pixel counts.

Both the compression algorithms used to save ballot images and the file formats are different for the poll level (CF200 series) and central count (CF500 series) tabulators. On the CF200 series tabulators, the images of all scanned ballots are compressed using run length encoding (RLE) and stored as a BMP files. Since the images are binary (black and white), RLE is very efficient in compressing the images up to 15 times. On the CF500 series tabulators, TIFF LZW (Lempel Ziv Welch) is used for image compression to save all scanned ballots. TIFF LZW is the de-facto standard for lossless image storage. LZW is the most popular compression for black and white and grayscale images. This algorithm compresses and decompresses without any information loss, achieving compression ratios up to 5:1.

From a software point of view, Democracy Suite includes several software modules for automation of paper-based voting. Election Event Definition modules include Election Event Designer and Ballot Designer features. While first one is used for collection of contest and candidate names, as well as administrative electoral divisions, the second one creates ballot styles and layouts using predefined ballot templates. This complete set of information is used for creation of binary voting configuration files for programming of voting channels. Another set of software automation tools are used for result tallying and reporting. These modules are responsible for election results acquisition from various voting channels, manual results data entry, results tallying, verification, auditing and reporting. Each voting channel produces the results information file in a common binary format. After importing these result files into the Results Tally and Reporting module, votes cast are stored in a temporary database giving the electoral officers the opportunity to perform results verification before making results public. This verification can be selectively performed either for all contests or just for contests flagged as critical. Finally, in an auditing process using a random algorithm, electoral officers and scrutineers can select ballots for inspection and compare images of scanned ballots with system recordings. Using this approach, a very high level of acceptance is achieved in the overall tabulation validity.

6 Electronic Remote Voting

Electronic Remote Voting (Internet voting) has some unique requirements that differentiate this method from traditional paper-based voting processes. In recognition of these unique requirements, a 5-step process was defined as shown in the following diagrams.

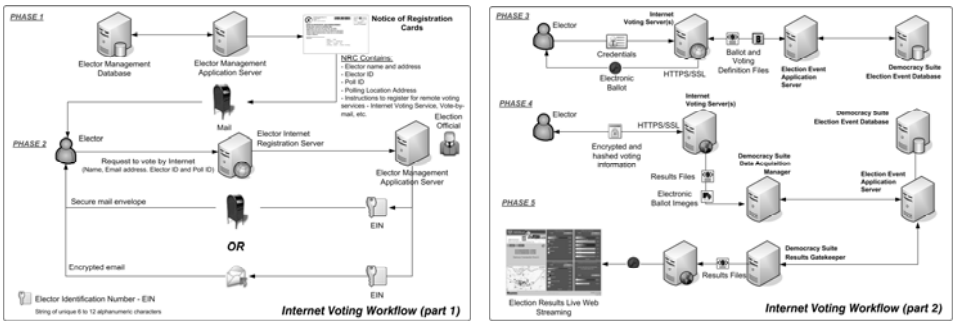

Figure 6: Internet voting five step process.

Phase 1 – Elector Management - This phase is common for any type of election, regardless of the voting method(s) being employed. At the end of the elector management process, the system generates the invitation to vote (NRC) cards to be mailed to eligible voters. Each NRC card contains information about the voter including name and address, unique elector identifier (Elector ID), etc.

Phase 2 – e-Voting Registration - Upon receipt of their NRC cards, voters can choose to vote using a traditional paper ballot at the polling location, or to register to vote using the Internet voting. If an elector chooses to vote via the Internet, they must first register at the designated Internet site (Internet Registration Server). Based on this information, the system generates a unique Election Identification Number (EIN) for that elector. This EIN serves a similar purpose to that of the PIN numbers commonly used in Internet banking. This number is communicated to elector using the secure mail service.

Phase 3 – Electronic Ballot Download - On the Election Day(s), electors who received EIN codes can access the Internet Ballot Issuing Server and proceed with voting by downloading an electronic ballot. Every electronic ballot is generated dynamically by mapping elector information with content in Election Event database. In addition, each ballot contains a randomly generated Ballot Activation Code (BAC), which is embedded into the ballot in the form of 2D barcode matrix. This code ensures that one ballot is issued and cast only once.

Phase 4 – E-Voting – A sample electronic ballot is presented in Figure 7. Electronic ballots can have animated help, configurable marking options (square, oval, circle, arrow, x, check mark, etc.), audio capabilities, magnification features, etc. This is especially important for visually impaired people who can vote using these special features. The voting process itself is identical to marking a paper ballot. After making a selection, the elector presses a Submit button which is followed by a confirmation screen. Depending on configuration settings, this system can prompt an elector to correct his selection if the ballot is blank, overvoted or undervoted. After elector acknowledgement, votes are extracted from the ballot and serialized to the Internet Voting Server over the secure communication link. At this point, the used EIN code is destroyed and the elector voting state is appropriately changed. For each electronic ballot cast, electronic image of the ballot is created. Using this approach, even electronic voting can have auditing trail (images can be printed and used as the paper ballots) and in case of a recount, the electronic voting process does not have to be repeated (generated images can be scanned using optical tabulators together with other paper ballots).

Phase 5 – Results Tally and Reporting - The results processing and reporting phase is the same for all methods of voting, including Internet voting and traditional paper ballot voting. The Internet Voting Server produces results files in the same format as those produced by the paper ballot tabulator devices.

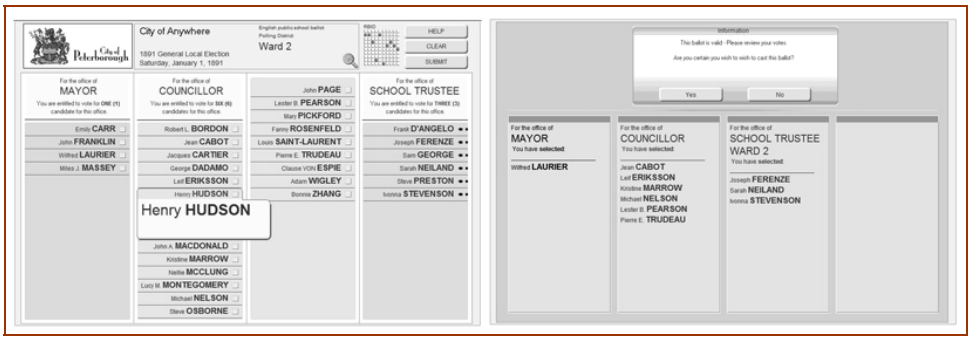

Figure 7: Sample electronic ballot with zooming feature.

7 Reporting

All reports can be divided into the following groups:

a) Election Event Definition reports provide information about the structure of the defined election event, with all of their election entities and their relations.

b) Elector Management reports include all of the information about the list of eligible electors, issued and mailed NRCs, status of electors (list of voters who voted at advanced polls and regular election days), list of issued certificates to vote, list of issued proxies, etc. The system keeps track of all electors who have registered to vote by Internet, along with their voting status.

c) Internet Voting Services status reports provide information about electronic ballots issued, along with the status of the Internet servers and connections, alarms (if any), etc.

d) Election Results Tally and Reporting module produces up-to-date PDF/Excel/XML reports in addition to the live web streaming reports, based on rich-content data representation (maps, tickers, charts, grids). Live web reports are fully customizable in terms of content and layout (Figure 8, left), providing interactive and dynamic results representation format at the election night (Figure 8, right).

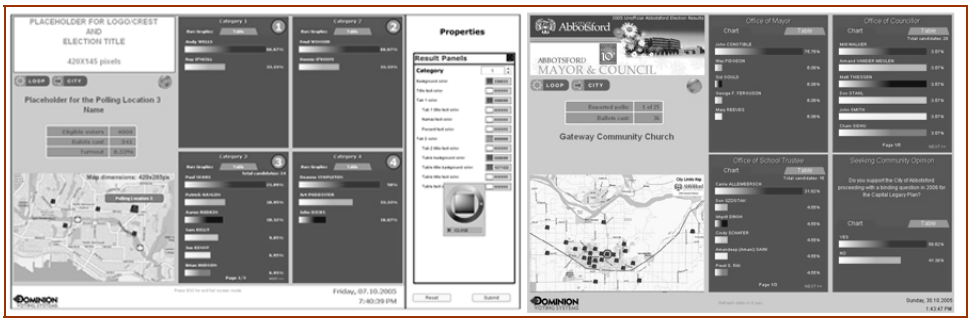

Figure 8: Live web streaming election results presentations.

8 Conclusions

In this paper we have presented automated election workflow based on Democracy Suite line of software and hardware products. Democracy Suite has a range of features to handle contemporary election issues. Computer technologies are utilized in order to provide ballots in a greater variety of formats to reach a larger percentage of electors. High migration is handled more effectively with database tools for elector list management. Automation is introduced into the poll to provide assistance to electors and also to support more complicated ballot styles. All security concerns for both internet ballots and election management have been addressed to ensure system integrity. Full attention is granted to election event and election cycle entities to minimize the required time required to stage an election. Our current work includes additional system improvements for making the Democracy Suite fully compliant with [FEC05] specifications.

Literature

[EML05] OASIS: EML (Election Markup Language) Schema Descriptions – Version 4.0., 2005.
[EA05] Election Act, Canadian Government, 2005.
[FEC02] Voting Systems Standards, Federal Election Commission, USA, 2002.
[FEC05] Voluntary Voting System Guidelines, Federal Election Commission, USA, 2005.
[HAVA02] Help America Vote Act, Federal Election Commission, USA, 2002.

Session 6: Observing E-Voting

A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament

João Falcão e Cunha, Mário Jorge Leitão, João Pascoal Faria,
Miguel Pimenta Monteiro, Maria Antónia Carravilla

Faculdade de Engenharia da Universidade do Porto
Rua Dr. Roberto Frias
4200-465 Porto, Portugal
{jfcunha | mleitao | jpf | apm | mac}@fe.up.pt

Abstract: In the 2005 Portuguese Parliament General Elections there were non-valid experiments of e-voting at five voting places and also through the Internet. *Faculdade de Engenharia da Universidade do Porto* audited such experiments. Relevant *security*, *transparency*, *usability* and *accessibility* evaluation criteria and sub-criteria were defined, and an auditing procedure based on AHP was established. This paper shortly presents the methodology used, the four e-voting systems and the main results of the overall experiment. The systems could be used successfully and were extremely popular with voters. However, more information to the citizens and to the officials involved in the e-voting process would be required for a valid election. The systems also need to be improved, for instance, to make sure that the number of votes electronically cast is the same as the number of voters that were validated and actually registered to vote at any particular site on the Election Day.

1 Introduction

1.1 Context

During the previous elections for the European Parliament, in 2004-06-13, and for the general elections for the Portuguese Parliament, in 2005-02-20, the government and the parliament agreed to carry out a set of experiments on electronic voting.

For the European Parliament elections there were 9 boroughs involved, geographically and socially dispersed, some in large towns with highly educated voters, and some in small villages with pensioners having little contact with technology. From a total 52 000 electors who cast a valid vote, 9 359 voted electronically (18%) [FE04].

For the elections for the Portuguese Parliament the selected boroughs corresponded to the 5 sites where the President of the Republic and the leaders of the political parties represented at the parliament voted. As Portuguese citizens registered to vote abroad could do it by postal vote (remote vote allowed), it was also decided to set up an Internet voting system. In all cases e-voting was voluntary and not valid, and who cast their vote traditionally was invited to also vote electronically. From a total of 26 515 electors who cast a valid paper vote, 8 824 also voted electronically (33%). From a total of 148 159 electors outside Portugal who were registered to vote by mail, 36 391 voted by mail (25%) and 4 367 voted through the Internet (12% of mailed votes) [Pi05]. After voting, each citizen was personally interviewed by an independent organization in order to collect an opinion about the experience (see below). In the Internet case, the voter could fill in a questionnaire for the same purpose.

Several public and private organizations were involved, but UMIC www.umic.pt, a special government unit with the overall mission of promoting innovation, was in charge of coordinating the project. CNE www.cne.pt and STAPE www.stape.pt, the public entities that oversee and manage general elections in Portugal were also deeply involved. CNPD www.cnpd.pt, a parliament controlled but autonomous unit that oversees the use of information and databases with personal information was also asked to audit and certify procedures. INDRA, MULTICERT, NOVABASE and UNISYS provided the e-voting systems (EVS) for the experiment. MULTICERT, under the guidance of UMIC and CNPD also had the overall responsibility of putting together a digital electoral register for all voters involved in the experiment, and to deploy such system during Election Day at all sites.

The experiments were very successful from the point of view of the voting citizens [OS05]. According to the exit interviews, 99.2% of the citizens that voted electronically enjoyed the experience and 98.1% said they would vote electronically in future elections; 80.5% trust the security of the EVS; 84.5% of the voters that had a paper trail option in the EVS used, consider important that the vote had been printed in paper and automatically inserted into a box; 86.3% consider that if such systems allow people to vote from other places then more people would vote. For people voting through the Internet the results were similar: 99.2% enjoyed the experience and 98.3% said they would vote in this way in future elections; 57.8% trusts the security of the EVS, 7.9% thinks it is not secure, and 34.3% do not know or do not answer the question. Regarding the security of Internet voting, only 1.7% thought it is totally secure against attacks from hackers, while 54.3% do not know or do not answer [UM05].

In order to guarantee the transparency of the process, Universities were invited to make proposals for auditing the process. In the case of the elections for the European Parliament five Universities were involved. Given the fact that it was difficult to manage so many auditors, UMIC agreed that for the Portuguese Parliament's elections there would be a call for tenders regarding the auditing process. *Faculdade de Engenharia da Universidade do Porto* (FEUP) was selected as the main auditor, on the basis of the quality of proposed work, experience and qualifications of the auditing team, price and schedule of work.

1.2 The voting experiments

Five e-voting sites were set-up requiring voters to go to the voting place. One of these sites had six e-voting places allowing the citizens to vote outside their traditionally appointed paper voting place. An Internet system was also deployed to allow e-voting from Portuguese voters registered as residing abroad.

Figure 1 describes the general set-up for the experiments during the Portuguese Parliament's elections.

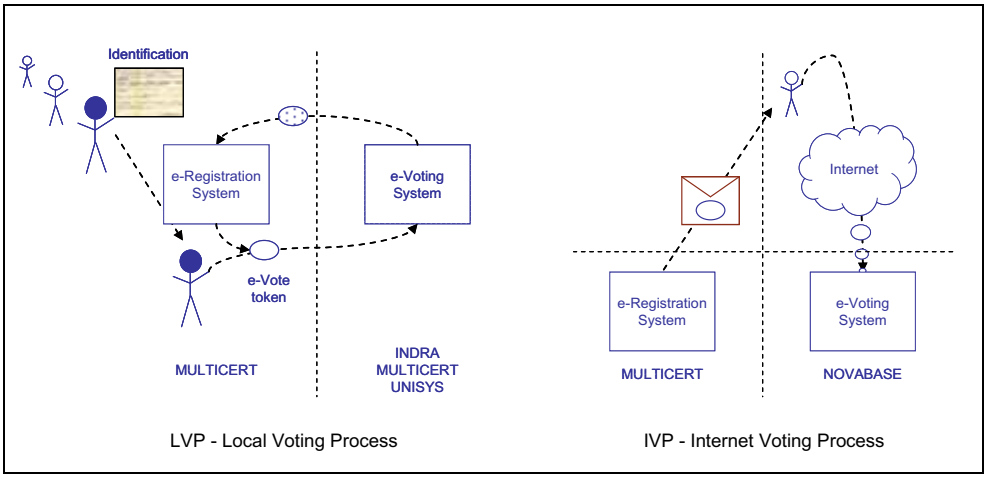

Figure 1: LVP: a citizen with a proper identification gets a token at e-Registration and then can vote. INDRA had one token for each voter, but in the other systems the token is reused after a new permission is granted. Number of voters and votes are counted both at e-Registration and at the e-Voting system. IVP: a citizen that is registered to vote gets an envelope by mail with a token (username and password). He may then log into the e-voting system.

2 The Auditing Methodology

The objective of the auditing methodology was to produce a thorough report on each EVS and to apply scores for each one on the criterion defined by UMIC: Security, Usability, Transparency and Accessibility.

Due to the characteristics of the process, there were 14 auditors involved. This is a large number, and there is a strong need to obtain scores for the EVS that consistently reflect the views of the group as a whole, and not just 14 different views. In order to simplify the assessment, the 4 criteria were decomposed into several sub-criteria. The Analytical Hierarchy Process (AHP) ([Sa80], [Sa87]), which is based on the comparison of the importance of each pair of sub-criteria, was the tool used to obtain weights of each sub-criterion under each criterion, aggregating the views of all the auditors.

2.1 Team composition

The auditing team members' had deep technical and management expertise. They had doctorates in Computer Science, Telecommunications, Security and Information Systems. There was 1 overall coordinator, 4 auditing teams with 3 or 4 elements each (as there were 4 different EVS), and 1 team with 2 elements, both with doctorates in Operations Research, that acted as facilitators during the whole process.

2.2 Phases of the process

The methodology followed by FEUP had three phases, corresponding to the periods before, during and after the Election Day.

Before the Election Day the team met several times in order to make decisions on the criteria and sub-criteria, on the assignment of the auditing team members to the e-voting systems (EVS) and voting periods, and on the set of questions and requests for information to send to each company.

At the Election Day, in order to make possible a comparative classification of systems for the same criteria and sub-criteria, each auditor visited at least two different EVS. There was always an auditor at each voting site, observing the opening moment, the voting process and the final closure, including the vote counting and the communication of results to the counting centre. There was also an auditor at the counting centre.

After the Election Day the auditing team had also at least one meeting with each company, in order to ask further questions that did arise during the audit. With all the information on-hand the auditing team had a long final meeting, facilitated by the Operations Research team, to discuss the scores given for each EVS on each sub-criterion. Taking into account all information, a report on each EVS was produced and sent to UMIC and then to each company.

The procedure for auditing the Internet EVS was adapted from this one as there was not an Election Day but an election period of several weeks. Such votes could only be counted after the postal votes were counted, two weeks after the actual Election Day.

2.3 The evaluation criteria and sub-criteria

The evaluation criteria (Security, Usability, Transparency and Accessibility) were defined a priori by UMIC. During several meetings that took place before the Election Day, the auditing team agreed on the sub-criteria under each one of the evaluation criteria (see Figure 2), based on [Ne93], [BH04], [Ca04], [Me00], [Mo01] and [Pi04]. These meetings were very important for the auditors to discuss and get a consensus on the meaning of each sub-criterion. As, during the Election Day, the teams could not meet and discuss the evaluation criteria it was necessary to promote a discussion on the criteria and sub-criteria with all the auditors, in order to obtain homogeneous evaluations.

SECURITY (S)		100,0%
S1	Audit-ability	10,3%
S2	Operator authentication	4,4%
S3	Certify-ability	9,0%
S4	Reliability	9,8%
S5	Detect-ability	4,6%
S6	Availability of system	5,4%
S7	Immunity to attack	8,1%
S8	Integrity of votes	14,4%
S9	Invulnerability	9,3%
S10	Traceability	3,8%
S11	Recoverability	5,3%
S12	Fault tolerance	4,6%
S13	Isolation	2,6%
S14	Security of communications	8,3%

TRANSPARENCY (T)		100,0%
T1	Anonymity	11,3%
T2	Atomicity	7,0%
T3	Authenticity	11,5%
T4	Trust	6,2%
T5	Technical documentation	2,2%
T6	Integrity of personal	2,8%
T7	Integrity of system	6,0%
T8	Non-coercion-ability	10,5%
T9	Precision of system	7,6%
T10	Privacy	7,6%
T11	Singularity (non reuse)	10,7%
T12	Transparency of process	3,5%
T13	Transparency of system	3,9%
T14	Verifiability	6,5%
T15	Separation of roles	2,9%

USABILITY (U)		100,0%
U1	Easiness of use	38,4%
U2	Speed of use	10,1%
U3	Clarity of language in interface	23,4%
U4	Localisation of interface	11,1%
U5	Emotional satisfaction	17,0%

ACESSIBILITY (A)		100,0%
A1	Convenience	14,4%
A2	Right to vote	47,0%
A3	Documentation for the elector	7,6%
A4	Flexibility	11,9%
A5	Mobility	19,1%

Figure 2: Criteria and sub-criteria for auditing, with relative weights [FE05].

As an example, the sub-criterion "Availability of the System" was described as "During the voting period, the EVS must always be available for all the actors, particularly the voters, in order for the process to run normally". Again as an example, a score of 1 would be given to an EVS that could work during the whole election day, if nothing wrong happened, a 3 if the system would for instance include a battery, that would allow it to work for at least 30 minutes without external power supply, and a 5 if the system would work, based also on batteries, during the whole election day. Such concrete guidelines are not always possible to define, but are desirable for consistent evaluations.

During those meetings it was also necessary to obtain the weight of the sub-criteria under each criterion. The tool used to obtain these weights is called Analytical Hierarchy Process (AHP) and is based on the comparison of each pair of sub-criteria by their relative importance. Every team-member had to fill-up a matrix (see Figure 2) comparing each pair of sub-criteria under each criterion. A 1 means the sub-criteria are equally important, a 9 means, for instance, that "Right to vote" is extremely more important than "Flexibility". The pairwise comparison matrix for each criterion was obtained by calculating the average of the answers of the team members. The AHP methodology was then applied to each criteria matrix leading to a balance of the sub-criteria under each one of the 4 criteria.

Accessibility	A1 Convenience	A2 Right to vote	A3 Documentation for the elector	A4 Flexibility	A5 Mobility
A1 Convenience	1	1/7	6	9	1/6
A2 Right to vote	7	1	9	9	8
A3 Documentation for the elector	1/6	1/9	1	1/6	1/8
A4 Flexibility	1/9	1/9	6	1	1/7
A5 Mobility	6	1/8	8	7	1

Figure 3: Matrix for the pairwise comparison of the sub-criteria of the Accessibility criterion.

After the Election Day, the auditing teams met to evaluate each EVS on each sub-criterion. This evaluation was given simultaneously to all the EVS after a general discussion and an agreement of the auditors involved. The score of each EVS under each criterion was obtained by calculating the internal product of scores with the weights of the sub-criteria under each one of the 4 criteria. The final result is shown in Figure 4.

	UNISYS	INDRA	MULTICERT	NOVABASE
Security	4,2	4,1	2,6	3,6
Transparency	4,2	4,3	3,2	3,0
Usability	4,2	3,9	2,7	3,8
Acessibility	3,7	3,3	3,5	3,6

Figure 4: Final evaluation under the 4 criteria of the 4 EVS (scale 1-5).

3 The e-Voting Systems and Associated Processes

The e-voting experiments involved hardware and software from 4 enterprises: MULTICERT, UNISYS/ESS, INDRA and NOVABASE. As mentioned in the introduction, MULTICERT developed the elector registration system used in all experiements and NOVABASE developed the Internet voting system. There were two kinds of presential voting systems: The *local voting* systems required that voters would go to their traditional voting place. This was the only location where they could cast their electronic vote. In the *local voting with mobility* system the voter could choose one from several places where to vote, all located in the same borough. All systems are shortly presented in the next sections. For further details see [FE05].

3.1 INDRA – Local Voting

The system proposed by INDRA is named Point&Vote. It consists of special purpose equipment based on a standard PC platform equipped with a touch screen with side view protection, a smart card reader and an internal printer for reports. The unit is portable and must be placed on top of a table. Two alternative versions were available, one with headphones and mouse for physically impaired voters, and another with a printer, where votes could be seen for a few seconds by the voter, but could not be removed from the collecting basket. This version was intended for evaluation of the need of a paper trail.

In order to vote using the INDRA system, each citizen receives a smartcard. This token is required to enable the use of the actual voting machine were votes are cast (and counted at the end of the Election Day). After being used the smartcard is returned to the e-registration and is not used again at the current election.

At the end of the voting period, each Point&Vote machine is closed with the operator (supervisor) smartcard and password, thus disabling any further voting action. Results from each machine can now be locally printed and transmitted subsequently over the internal modem via a secure communications link to a computer of the Central Election Authority.

3.2 UNISYS/ESS – Local Voting

The system proposed by Unisys and manufactured by Election Systems and Software (ESS) was the iVotronic. It can be generally characterised as a touch screen voting unit, portable and easily configurable (height and orientation), with good privacy protection. These features, plus an optional audio interface, allow good support to visually impaired and wheelchair locomoting voters.

The PEB (Personal Electronic Ballot) is the token that gives access to one vote in the iVotronic machine, prevents overvoting, and notifies the voter in the case of an incomplete operation (such as removing the PEB from the iVotronic unit before pressing the physical VOTE button). It's a sealed unit communicating within a very short range through a proprietary infrared technology and protocol that was designed to prevent communication with standard IrDA transceivers. After each use the PEB must be regenerated in a specific machine with the proper infrared interface.

Some special operations can be performed using a different supervisor PEB requiring explicit password validation. If validated, operations such as opening a voting session (zeroing the counters), closing the voting session, or casting or eliminating incomplete votes (when the voter didn't press the VOTE button), are allowed and logged. During the voting session results are accumulated internally and redundantly recorded (in 3 different flash memory units). All operations, including the supervisor actions, are also timed and logged.

At the end of the session the voting units must be closed and its accumulated results transferred and added to the supervisor PEB memory, allowing several units to be combined in a single one. This PEB is then read in another machine, which also can combine several results. This machine can now print the results (totals and partials) and transmit them to a computer of the Central Election Authority using a modem and a phone line.

3.3 MULTICERT – Local Voting with Mobility

Differently from the previous systems, the MULTICERT voting system allowed citizens to vote electronically in a place different from their traditional one, within the same borough. In the future, the goal of the system is to allow citizens to vote in any other borough.

This was achieved by a distributed e-registration system, based on a central database that stored information about what electors had already voted, and was remotely accessed by client applications located in each place.

Another distinguishing feature of this system was the existence of an electronic ballot box system (EBBS) that actually stored the electronic ballots, separated from the electronic voting units where the electronic ballots were filled in. Small i-button devices were used to carry authorizations (similar to empty ballots) from the EBBS to the electronic voting units, and carry back filled in ballots to the EBBS.

Besides a touch screen, each electronic voting unit had a small printer to print and store paper ballots corresponding to the electronic ballots, with the purpose of enabling non-electronic ballot recounting and improving the confidence on the process. The elector could check by visual inspection that the printed ballot corresponded to his electronic ballot.

Special operations could be done in the EBBS using supervisor i-buttons, namely start a voting session (zeroing the counters), close the voting session, and subsequently view on screen, print and export the results. The results were not transmitted electronically.

3.4 NOVABASE – Internet

The Internet voting system was aimed at all the citizens registered to vote outside of Portugal using postal vote. Two separate mailings were sent to voters abroad: the one containing the valid ballots and another one with the information and keys to allow the vote using the Internet system. The Internet voting process (i-voting), had the following steps:

1. Using a database of electors the system generates individual credentials for each one, a unique code of a username and a password.

2. The electors' information is registered together with the credential in the Active Directory of the central system.

3. The credentials are posted to the electors abroad by mail. The message does not include the elector number, to prevent other people to vote.

4. Pairs of encryption keys are generated. The public key is send to Novabase to be stored in the Database. The private key is divided into 7 parts, one for each political party represented. Votes can only be read with these 7 keys.

5. The vote process is open, allowing browsers to access the server. In the experiment this server was located at the headquarters of Novabase.

6. The elector receives the credentials. He/She can use any computer with a browser, able to accept some JavaScript and cookies, to access the web page www.votoelectronico.pt. He/She has to introduce the elector number and the credential. If all is correct, he/she can then proceed to vote.

7. The confirmed vote is registered in a database table, using two key encryption. The public key is used to encrypt. During the same transaction it is stored that the citizen has voted in the credentials table and in the Active Directory. Afterwards the elector is informed that the vote has been confirmed.

8. At closure of the election the information in the Active Directory is printed and sent to CNE. The Active Directory is erased in the presence of CNPD. A copy of the database is stored and sealed in a CD with a MD5 seal, kept by UMIC.

9. Counting of the votes is done with a special application. As the votes are encrypted it is required to bring together the 7 keys to produce the final result.

The system uses traditional client server architecture. From a logical point of view there is one Web site and clients over the Internet. The Web site is in fact divided in two parts: an http information site and an https secure one, with the forms and vote registration.

4 Conclusions

It is widely accepted that there is very high satisfaction and trust with the current paper based electoral process in Portugal. Most of the citizens cannot evaluate the security or transparency of the computing and communication systems to be eventually used in elections. Certification and audits are therefore required to provide a wide socially recognised guarantee of security and transparency for the new systems and processes.

The audit identified many advantages and problems of the several EVS. One of the problems observed has to do with the inconsistencies in the final number of counted electronic votes. In each voting site there were a number of total electronic votes Nv (counted by the EVS) and a total number of citizens Cv that were given tokens to vote (counted by the e-Registration system). The three situations below occurred. This could be a problem of the EVS, of the procedures people used, or both:

- Nv > Cv. At least one citizen voted twice. It could have happened that one citizen was given more than one chance to vote (e.g.; claimed token was faulty).
- Nv < Cv. At least one citizen did not vote. It could have happened that one citizen actually did not vote at the EVS (not a problem, if voluntary).
- Nv = Cv. All was fine, or pairs of the above happened at the same EVS.

All systems, except the Internet one, suffered from this problem. This can be a major problem facing the adoption of e-voting, and illustrates the need for improved systems and improved voting processes. Improved systems can make the voting process more secure and transparent, as well as more usable and accessible. Improved information to the citizens and to the officials running the election, are key requirements for maintaining trust and satisfaction with the democratic election processes.

The audit method presented did not produce a final ranking of systems. This would require that relative importance would be given to the 4 criteria. Acceptable minimum levels of performance on each criteria (or subcriteria) could have been defined. For instance, one may argue that EVS security level must be over a certain level in order to be acceptable to be used. Both of these decisions, on relative importance of criteria and minimum performance levels, must also involve political involvement.

An improved audit method could include a comparison of EVS with the traditional paper voting system, on the same criteria. Weak and strong points of each type of system could be compared under the same sub-criteria, if making sense.

Acknowledgments

The authors would like to acknowledge the work and contributions of Gabriel David, J. Correia Lopes, A. Carvalho Brito, J. Magalhães Cruz, Sérgio R. Cunha, R. Moreira Vidal, Henriqueta Nóvoa, J. Vila Verde, Miguel Gonçalves, L. Miguel Silva, and J. Fernando Oliveira. The auditing process benefited from contributions from Diogo Vasconcelos, Sara Piteira and João Vasconcelos, from UMIC, and from Fernando Silva, from CNPD. The authors would like to state their appreciation for the very professional attitudes of officials from CNE and STAPE, and from the representatives of all the enterprises that were directly involved in the experiments.

References

[BH04] B. Bederson, P. Herrnson: «Expert Review Plan of Voting Machines», Research Report, HCI Lab & Centre for American Politics and Citizenship, U. Maryland, USA, 2004.

[Bu04] T. M. Buchsbaum: «E-Voting: International Developments and Lessons Learnt», in [PK04], p. 31-41.

[Ca04] Jean Camp, Allan Friedman, Warigia Bowman (ed.): «Electronic Voting Best Practices - A Summary», Voting, Vote Capture & Vote Counting Symposium, Kennedy School of Government, Harvard University, 2004-06, 23 p.

[FE04] (in Portuguese) J. Falcão e Cunha (ed.): «Relatório Final de Auditoria – Eleições para o Parlamento Europeu de 2004-06-13» (Final audit report of the Portuguese electronic elections experiment for the European Parliament); 2004-08-04, FEUP, Portugal, 28 p.

[FE05] (in Portuguese) J. Falcão e Cunha (ed.): «Relatório Final de Auditoria – Eleições Legislativas de 2005-02-20» (Final audit report of the electronic elections experiment for the Portuguese Parliament); 2005-04-21, FEUP, Portugal, 78 p.

[Me00] Rebecca Mercuri «Generic Security Assessment Questions» (www.notablesoftware.com).

[Mo01] (in Portuguese) A. Monteiro, N. Soares, R. M. Oliveira, P. Antunes: «Sistemas Electrónicos de Votação» (Research Report supervised by P. Antunes, DI-FCUL TR–01–9), 2001, Dep. Informática, FCUL, Campo Grande, 1700 Lisboa, Portugal.

[Ne93] Peter G. Neumann: «Security Criteria for Electronic Voting», 16th National Computer Security Conf. Baltimore, Maryland, 1993.09.20-23.

[OS05] (in Portuguese) OSIC – Observatório da Sociedade da Informação e Conhecimento «Voto Electrónico - 2.ª Experiência Piloto de Voto Electrónico Presencial, Resultados Eleições Legislativas de 2005-02-20», 2005-03, 22 p.

[Pi04] (in Portuguese) R. R. Pinto, F. Simões, P. Antunes: «Estudo dos Requisitos para um Sistema de Votação Electrónica» (Research Report supervised by P. Antunes, DI-FCUL TR–04–2), 2004, Dep. Informática, FCUL, Campo Grande, 1700 Lisboa, Portugal.

[Pi05] (in Portuguese) S. R Piteira: «Projecto Voto Electrónico», Voto Electrónico e Defesa da Privacidade Workshop (Electronic Voting and Privacy Protection Workshop), CNPD, Assembleia da República, Lisboa, 2006-12-07, 21 p.

[PK04] A. Prosser, R. Krimmer (Eds.): «Electronic Voting in Europe – Technology, Law, Politics and Society», Lecture Notes in Informatics, GI-Edition, 2005.04.23, 182 p.

[Sa80] T. L. Saaty: «The Analytic Hierarchy Process». McGraw-Hill, New York, 1980.

[Sa87] T. L. Saaty: «The Analytic Hierarchy Process: what it is and how it is used», Mathematical Modelling, 9, 1987.

[UM05] (in Portuguese) «Voto Electrónico - 1.ª Experiência Piloto de Voto Electrónico Não Presencial, Resultados - Eleições Legislativas de 2005-02-20», UMIC, 2005-03.

Voting in Uncontrolled Environment and the Secrecy of the Vote

Kåre Vollan[1]

Quality AS
P.O. Box 5153 Majorstua
NO-0302 Oslo, Norway
kvollan@online.no

Abstract: Voting in uncontrolled environment either by post or by the Internet is about to be made generally available in many countries. The main purpose is to increase participation at times when the voter turnout is generally decreasing. Electronic voting both in or outside controlled environment offers advantages in producing fast and reliable results and long term cost savings in the conduct of elections.

A number of problems relating to security, reliability and general trust can be solved by Internet voting, once an infrastructure for voter identification is in place. However, neither postal votes nor Internet votes can guarantee that the vote is cast in secrecy without intimidation or pressure. Even without the most serious violations to a free vote, the pattern of voting will change and the concept of voting being a strictly personal and secret act is likely to be weakened over time.

There are few reasons to doubt that the introduction of voting by Internet once generally available will have the same success in terms of usage as other Internet services such as bank transactions, tax returns etc. Once being implemented in a user friendly and reliable manner the electronic interface may within foreseeable future become the major voting channel.

This paper does not discuss in depth the legal issues related to whether uncontrolled voting meets international commitments regarding a secret vote. The focus is to what extent the most likely change of voting pattern from a public to a more private, but less secret event, is a positive development. It concludes that the problematic issues which can be raised are fundamental and the long term damage to the perception of a personal and secret vote should be discussed by governments and inter-government organisations. Alternatives such as electronic voting in controlled environment prior to election day may, to a large extent, serve the same purpose without showing the negative side effects of voting outside of controlled environment.

---

[1] The author is a consultant on electoral issues providing advice mostly in post conflict countries and in countries in transfer to democracy. He has also headed a number of international election observation missions and he is a registered IT quality auditor (IRCA).

1 Introduction

1.1 Trends in Voting Methods and Voting Behaviour

The international trend of decreased turnout in elections has led a number of countries to offer possibilities of voting outside of polling stations on election day. The main class of alternatives is variants of early voting (voting before election day) either conducted in controlled environment where the voter has to meet in person and election officials will check that the vote is cast in person and in secrecy or cast in uncontrolled environment by a postal vote or a vote by Internet. In addition voting may be offered to bedridden people by use of mobile teams on or before election day and remote voting may be available even on election day.

Increasing voter participation is clearly the main reason used to offer early voting in various forms, but other reasons will also be discussed below. Early voting in controlled environment is common for example in Scandinavia. In Norway around 20% of all votes cast in the last elections have been early votes [NO00]. Postal votes were first introduced to accommodate groups which would otherwise be disenfranchised such as voters travelling or living abroad or voters with disabilities making it difficult to come to a polling station. However, postal voting has in some countries such as Switzerland, Great Britain and Spain been offered to voters in general. In the general elections in 2005 in the UK the share of voters requesting a postal ballot was 12.1% up from 8.3% during the European Parliament and local elections in 2004 [UK01].

Voting by Internet has been offered in some countries such as Switzerland (in some cantons) and Estonia. In November 2005 23% of all votes cast in the municipalities with the possibilities for Internet voting in Geneva used that possibility. During the 2005 local elections in Estonia less than 2% of those voting cast an Internet vote [NO00].

A number of countries are assessing the possibilities for introducing voting by Internet. The main concern has been the reliable voter identification together with the secure technical implementation of such systems. Public systems for electronic signatures[2], which will help solving some of the security issues with Internet voting, are being introduced. If such public systems are regarded sufficiently secure for bank transactions and public services in general at least the highest security level offered for such services would suffice even for voting. Once the security requirements have been met it is likely that Internet voting will be proposed in a number of countries in the years to come. Once introduced it may show the same effect as other Internet based services and a major share of the votes cast may be Internet votes but whether Internet voting will increase the total turnout or just replace other means of voting remains to be seen.

[2] PKI – Public Key Infrastructure.

The Council of Europe has assessed electronic voting in uncontrolled environment against international obligations and commitments in the Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting [CE03]. The recommendation states:

> "Bearing in mind that the right to vote is one of the primary foundations of democracy, and that, consequently, e-voting system procedures shall comply with the principles of democratic elections and referendums;
>
> Recognising that as new information and communication technologies are increasingly being used in day-to-day life, member states need to take account of these developments in their democratic practice;
>
> Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;
>
> Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:
>
> – enabling voters to cast their votes from a place other than the polling station in their voting district; …"

When discussing the international commitments the recommendation says:

> "IV. Secret suffrage
>
> 16. E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.
>
> 17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.
>
> 18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.
>
> 19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote. "

The secrecy of the vote is only discussed in the technical context in the paper: The system need to be designed in such a way that individual votes cannot be identified once the result is established. The conclusion has also been shared by the Venice Commission [CE03]:

> "1. In conclusion, remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either non-supervised postal voting or electronic voting."

The fact that the voter may not be alone when casting the vote is much less prominent in the documents from the Council of Europe. This is a fundamental feature of both Internet and postal voting. Even if the vote once cast cannot be traced to the voter, the secrecy of the vote cannot be guaranteed. So far international observer missions and organisations have concentrated on security issues and much less on problems related to votes cast in groups with possibilities for undue pressure and even intimidation.

There is not full international agreement to whether uncontrolled voting complies with the requirements for secret votes. A number of countries have decided to be restrictive in offering such possibilities and if the do it is only offered to groups of voters who would clearly otherwise be disenfranchised. Other countries have decided to open such possibilities for all voters and their view is that the voting still complies with international standards as long as a controlled alternative is offered. This paper will not discuss the legal aspect of the question in full depth even though the international commitments are listed below. The subject for this paper is rather to what extent the development towards more uncontrolled voting is a positive development. By offering voting in uncontrolled environment to voters in general the concept of elections is being changed without a thorough discussion of the most likely end result: Voting may not be a secret act any more but may be carried out by voters sitting together, in families, in groups of young people, in community centres etc. This may open the vote for intimidation, trade with votes etc. But even if the most serious violations will be limited the effect over time may be that the concept of a personal, secret vote is weakened.

1.2 Types of Voting

Direct elections to national and local representative bodies have traditionally been conducted in polling stations during one or few election days. Polling station staff ensures that the vote is cast in person and in secrecy free from intimidation and pressure of any kind. Under various conditions many countries have allowed for early voting, postal voting and recently voting over the Internet.

It is common to differentiate between the following types of voting:

a. Voting in controlled environment, means any voting where election staff overlook the process of casting the ballot. This may happen in a polling station on election day or in a particular site for early voting.

b. Voting in uncontrolled environment either as a postal vote or by the Internet. In these cases it is up to the voter to secure the physical environment under which the ballot is cast.

The ballot may be a paper ballot or an electronic ballot. In addition the vote is conducted in phases:

a. The phase prior to elections day, the early voting
b. The election day(s) voting.

Voting types may be illustrated by the following matrix [NO01]:

	Controlled		**Uncontrolled**	
	Early voting	**Election day voting**	**Early voting**	**Election day voting**
Paper	At defined sites with regular paper ballots	Traditional polling stations with paper ballots	Postal votes	Postal votes
eVoting	Voting machines at defined sites	Voting machines in polling stations	Internet Voting	Internet Voting

Figure 2: Overview of types of voting

2 International Commitments Related to the Types of Voting

According to broadly accepted standards election should be *universal, free, fair, secret* and *transparent* [OD04].

A *free* vote means that the ballot is cast in person free from intimidation and undue pressure. *Universal* means that every citizen who has reached a certain age and fulfil accepted criteria can cast a vote. *Secret* would mean that the person can rest assure that the vote will not and can not be disclosed to anybody. This does not prevent a voter from volunteer his or her choice but it should not be possible to verify the information given by the voter. *Fair* means that candidates run under the same conditions and their supporters have the same fair chance to take informed decisions and cast the vote. The requirement of being fair would also imply all votes should be counted correctly, the tabulation should be correct and the process protected against fraud and mistakes. The best guarantee against fraud and mistakes when using traditional technology is *transparency*. This is assured by the possibility for representatives of all stakeholders to witness every step of the process, from the voter enter the polling station to the protocol is drawn up and the results are tabulated. The only exception is when the voters are making his or her personal secret choice.

The different types of voting will score differently for each of the commitments, which the table below indicates:

	Controlled		**Uncontrolled**	
Commitment	**Paper**	**Electronic**	**Paper**	**Electronic**
universal	Medium	Medium	High*	Very High*
free	Very High	Very High	Very Low	Low
fair	Very High (-)	Very High (+)	Low	High
secret	Very High	Very High	Very Low	Very Low
transparent	Very High	Low (-)	Low	Low (-)

* The high scores are in particular set for situations where uncontrolled voting comes in addition to voting in the polling station, but may eventually deserve a high score even if uncontrolled voting were the only option.

Figure 2: An indication of how controlled and uncontrolled voting meets international criteria for elections.

The table is meant as an indication only. The rating clearly depends on how each type of voting is implemented. It is possible to conduct paper voting in a polling station without any transparency and one may improve transparency for electronic voting in polling stations by printing a paper which can serve as an audit trail. The rating should reflect situations where regular procedures are applied by an election management body (EMB; that be a ministry, an independent election commission or any other body charged with the overall election administration responsibility) in good faith in order of conducting correct elections.

Voting outside controlled environment is being used mainly to strengthen the *universal* quality of the vote. By requiring voters to meet in person in a polling station on election day, bedridden people, people with disabilities, people travelling etc may be disenfranchised. In addition some voters may just decide to go to the polling station, but they may choose to vote by mail or by Internet if given the chance.

The freedom and secrecy can clearly best be guaranteed when the vote is cast in controlled environment. This is the only place where officials can make sure that the vote is cast without undue influence of any kind.

A *fair* election would on polling day mean that the process works as intended. Even in traditional democracies the controls and checks have not always been implemented in such a way that deliberate attempts to cheat could be resisted. Often the identity of the voter is not checked, voting material may not be secured and the rules for secret voting may have been rather relaxed even in polling stations.

On the other hand in controlled environment the possibilities for preventing impersonation, intimidation and group pressure is obviously much better that if the voter has to secure his or her own environment. The possibilities of impersonation are much higher by uncontrolled voting, even though modern measures may help reducing the risk by Internet voting.

When the votes are cast by paper ballots and manually counted the process is slow and often inaccurate. Human errors are bound to happen and the verification procedures for disclosing mistakes may vary a lot. Electronic voting, in controlled or uncontrolled environment, has the big advantage of producing correct results fast.

A *transparent* election is secured in polling stations by a fairly simple and compressed process witnessed by observers and the general public. This does not mean that voting in polling stations is always flawless, but correctly implemented there is a paper trail from observed vote till the protocol is signed which can be witnessed and checked even after the elections. Electronic voting has a major disadvantage in that ballots are being stored as electronic information within the computer and the integrity of the vote and the count is only guaranteed by the IT-systems themselves. Measures can be taken to validate the systems and certification schemes may be established, and the requirement for transparency may rest more on the process of acquisition rather than the vote itself. However, all such measures are dependent on a genuine, general trust in the EMB [KV05] and [OB08]. Should the EMB have a will to manipulate the systems to produce a certain result, this can hardly be prevented by independent validation of the system. Validation would be on prototypes and only the EMB can guarantee that the systems used are exact copies of those being validated.

3 Challenges to Voting in Uncontrolled Environment

Uncontrolled voting by mail and by Internet faces severe problems both regarding security and secrecy. On the security issues electronic voting has clear advantages provided modern identification measures are implemented. However, there is no technology available to guarantee that the vote is cast in secrecy free of intimidation and pressure.

3.1 Postal Votes

Postal vote is possibly the most vulnerable method being used today. It has been used to accommodate groups which would otherwise be disenfranchised, but in some countries it has been offered to the electorate in general.

Allowing refugees to vote was an important feature of the election Bosnia and Herzegovina after the war ended in 1995. From 1998 such votes were done by mail. During the elections in 1998 and in 2000 blatant attempts of impersonation of voters were disclosed and even high officials were penalised for assisting in the fraud[3].

Great Britain has in the last elections allowed for postal vote on demand. That means that any voter can request a ballot be sent to his or her address and the voter returns it by mail. During the elections for the Birmingham City Council in 2004 postal voting was used to fraudulently change the results in the wards of Bordesley Green and Aston [BI09]. Persons involved were penalised and some candidates lost the right to stand for elections. A number of techniques were used to manipulate the postal vote, such as requesting the ballot to be sent to addresses where community leaders would fill them in and return them, theft of postal bags, reopening and changing ballots, etc. The election court[4] found that the "evidence of fraud was overwhelming".

3.2 Voting by Internet

Most of the most blatant violations from Bosnia and Herzegovina or from Birmingham could be avoided by a good security system implemented on Internet voting. Electronic voting in uncontrolled environment should, if correctly implemented, protect the integrity of the voting better than postal votes [NO00] and [KV05].

Postal votes may require a signature to an outer envelop and the signature may later be checked if one suspects irregularities. Electronic signatures are being introduced in a number of countries for use in Internet bank transaction, communication with authorities including tax returns etc. So far the most common way of doing this is by pin codes combined with permanent or dynamic passwords. None of these methods offers any guarantee that the person at the screen is the person given the codes, and it is accepted (regardless whether it is legal or not) that person may use an authorisation to actually operate the computer on somebody else's behalf.

Future technology will probably include keys with biometric identification, and at that point in time one may be able to check that the person with the authorisation is present at the computer, but there is no guarantee that the person is alone. In conclusion the practical measures taken against impersonation may be much stronger for Internet voting than by postal votes. The secrecy of the vote can, however, never be guaranteed by any uncontrolled voting.

3.3 International Conventions and Commitments

It is universally accepted that principles of suffrage require a State to establish a system of elections that ensures secrecy of the ballot. Article 25 of the 1966 International Covenant on Civil and Political Rights (ICCPR) provides:

---

[3] The author was Director for Election at the OSCE Mission to Bosnia and Herzegovina in 2000.
[4] In local government elections in Britain, an "election court" is a court consisting of one High Court Judge.

> (b) to vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors;

European conventions and commitments are consistent with the ICCPR. Article 3 of Protocol N°1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms similarly provides:

> The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure free expression of the opinion of the people in the choice of the legislature.

The Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, later the OSCE, (29 June 1990) states:

> (5) [The participating States] solemnly declare that among those elements of justice which are essential to the full expression of the inherent dignity and of the equal and inalienable rights of all human beings are the following:
>
> (5.1) free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure, under conditions which ensure in practice the free expression of the opinion of the electors in the choice of their representatives; …..
>
> (7) to ensure that the will of the people serves as the basis of the authority of government, the participating States will
>
> …
>
> (7.4) ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public;

These conventions and documents state the obligation of a State to hold free elections by a secret ballot.

Election observer missions to transfer democracies have normally commented upon breach of secrecy when being observed in polling stations. So-called family voting is common. This is voting where family members enter the secrecy booth together. There may be no sign of intimidation, but it is still reported as a violation of the rules. Observer missions have been less concerned with the possibility of team work when an uncontrolled ballot has been filled in, even though the aspect has been mentioned.

Some countries interprets the commitments to mean that all votes cast should be secret whereas other would hold it for sufficient if a controlled environment is being offered to all voters who want to cast a secret vote.

4 Aspects of a Secret Vote

Postal voting and voting by the Internet do not guarantee a secret vote. Even with strong instructions and guidelines, there will be no guarantee that a ballot has been filled in secret with the marked ballot out of the view of others. In the following various aspects of allowing for a non-secret vote are discussed.

4.1 Tracing Votes Cast in Paper Based Systems

A secret vote would mean that nobody witness any acts where the voter's choice is being made. In addition the system should insure that a vote already cast cannot be traced back to the voter.

In some traditions, e.g. in the UK and in some former British colonies, the ballots are numbered and the voter's name is entered on the ballot stub with a corresponding number. This enables election officials to trace votes of individuals after the elections. Such a tracking would be a serious election violation and the secrecy may be maintained in countries with an election administration with full integrity. The justification for the numbers is that it may be used when investigating petitions relating to election fraud, and only a judge can allow for the secrecy to be broken. As one of the few cases in recent years such a decision was issued in the UK during the investigation of the Birmingham case mentioned earlier.

If very small batches of ballots are accounted for it may be a breach of secrecy. Many countries would therefore have a minimum number of ballots (e.g. fifty) which can be counted in an identifiable batch.

For early voting or ballots cast in a polling station where the voter is not registered so-called tendered ballots are used to prevent multiple voting or to check the voting right of a non-listed voter. The ballot is called tendered because it is not immediately accepted. It will have to be verified against the voter register and against any multiple voting by the voter before being accepted. The ballot is put in an unmarked envelop which in turn is entered into an envelope where the voter's name and ID number and possibly a signature is written on the outside. During the count the outer envelope is checked against the voter registers and if it is accepted as a good vote the outer envelope is broken and the inner envelope is entered into a box. After the verification process the box is emptied, the ballots removed from the neutral envelopes and the votes are counted.

If the procedure is followed, the secrecy of the voters is maintained. This process can be observed by candidate representatives, but it also dependents on a certain level of trust. Checking certain voters' ballots would be technically possible, but clearly a serious election offence.

4.2 Why Secret Votes?

The reason for the secrecy is first of all that the vote should be cast without any interference, intimidation or pressure. The ballot is the voter's own personal expression of his or her will. Without having any way of checking what an individual has voted buying votes will be practically impossible, even though strong community leaders may be able to direct a village or neighbourhood without having the possibility to check each vote individually.[5]

The concept of a secret vote is so well rooted with most people in old democracies. During the upbringing, in schools and in participation in the civic society the secrecy of the vote is taken for granted. A very strong protection of the secrecy may not be felt to be needed any more because any voter who wants the secrecy be protected will be able to cast the vote free from pressure.

In transfer democracies so-called family voting (family members entering the secrecy booth together) used to be common. This did not necessarily mean that voters were intimidated, but the vote was clearly less personal than if cast in solitude. Not least by encouragement from observer missions and the international community in general stricter rules have been implemented in a number of countries. In the elections in the Palestinian territory in January 2005 and in January 2006 the training of election staff had improved tremendously compared to the elections in 1996[6], and family voting was reduced if not eliminated. The long term effect of a strict regime will hopefully be a more profound understanding of the personal responsibility every voter has for the vote.

In Russia and in Romania it was common in early elections after the change to multi party elections (1992 and 1993) to observe large groups of voters filling in the ballots together outside the booth, at least in some districts[7]. The reasons given could be the complexity and lack of light in the booth etc. Intimidation was not necessarily observed or reported, but obviously in such circumstances it would have been possible for a community leader (a mayor, a kolkhoz director etc) with his or her mere presence to control the voting.

In the cases above there may not be a strong wish by the voter to hide his or her vote from either a family member or from all other people present for that matter. On the other hand the environment does not demonstrate the personal nature of the vote and it does not encourage people to insist on a secret ballot.

The conclusion is that the concept of a secret vote is not an obvious one. In order of having the concept generally accepted the secrecy would have to be enforced.

---

[5] Examples of retaliation on a whole village or threats of the same has been observed in some countries though, e.g in Zimbabwe in 2003 and 2005 [KV06] and [KV07].
[6] See election observation reports from the EU and NDI.
[7] See the reports of the Norwegian Helsinki Committee on elections in Romania in September 1992 and in Russia in December 1993.

4.3 Effects of Non-Secret Votes

When discussing the uncontrolled vote as an offer to all voters one has to consider the variety of family structures and community structures that exist in any society. In the Birmingham case the judge wrote: "It should be merely noted that undue influence remains a huge and apparently irradicable problem with postal voting, especially in vulnerable communities, including some of those with ethnic minority electors" [BI09]. This is a comment not on the fraud which the case was concerned with but rather the general problem of a non-secret vote. The Birmingham case included minority communities with traditional family structures. The problem may, however, be valid in a large variety of families.

In a many families the *pater familias* (or any family head) may do all the paperwork and mark all ballots for the whole family, only asking family members to sign the forms or provide the electronic signature where required. Members of the household may accept this as a simple arrangement for paying bills, do tax return, etc and therefore fail to see a problem if the same arrangement is followed for voting. It could happen that a family member would want to cast an individual vote, but due to a traditional respect for the head of the family he or she would hesitate to demand to fill the ballot out in person and in secrecy. In addition to the possibilities of "family voting", there may also be possibilities for a coordinated effort by community leaders which go beyond legitimate assistance and which may include breach of secrecy.

This has a self strengthening effect: Voting will not have any focus in the family because the family head is always taking care of it. As a consequence political consciousness may be reduced and a wish for casting a secret vote may never be expressed, even when a family head would have no objection to it. The problem is not so much the cases where a family member insists on a personal, secret vote, but rather where the voting is seen as any other paperwork and does not get any special attention. The opportunity of building up consciousness about the basics of representative democracies is weakened or lost.

The main source for the understanding of a personal and secret vote has been the strict regulation of the vote in polling stations. Should this educational element be less prominent it may happen that new generations of voters would lose out on the personal aspect of the vote. The effects may be stronger for groups of immigrants from countries where family voting is an almost legitimate tradition even in polling stations, but the risk is there for all groups. Internet voting is often said to be more attractive for young people. If so, young people may then choose to vote together and a group pressure may easily develop.

4.4 Proposals to Reduce the Negatives Effects of Uncontrolled Voting

Some measures may be taken to reduce the negative effects of uncontrolled voting. One is to allow for uncontrolled voting only prior to the elections, not on election day (as in Estonia in 2005). In such case one may build into the system a legal possibility to regret the vote and to override the vote on election day in the polling station. This can be implemented by regarding the postal ballot as tendered ballot which has to be checked against the voter register and the votes cast on election day before being counted.

By early Internet voting the voter may be given a possibility to change his or her vote either on the Internet or by casting a ballot in person on election day. That would offer a possibility to such voters who might have been under pressure by family members, community leaders or friends to cast a particular Internet vote to override the vote on election day in controlled environment. This would only help in such cases where the voter is conscious enough to want to exercise the right to a secret ballot. To accommodate such a possibility technically, a link between the ballot and the voter has to be maintained until the final verification. The verification of whether the ballot is to be counted or if it is overridden by a later vote has to be done first. In the case the Internet vote is to be counted the link between ballot and voter is broken for good, and only then the vote can be counted. Such a system can maintain the secrecy of the vote provided any manipulation by insiders can be ruled out.

Should uncontrolled voting be common it is extremely important that strictly controlled polling stations are available on Election Day for all those who choose to cast a vote in guaranteed secrecy. The danger by a successful introduction of uncontrolled voting is that there is an administrative pressure to reduce the number of polling stations. One may also experience a more relaxed secrecy within the polling stations since the officials would know that the votes are generally not secret any more, even though the need is for more not less control in the polling stations.

A measure which is taken by some countries is to require that the voter, and sometimes even witnesses, sign a statement confirming that the vote is a personal one and that the ballot is cast in secrecy. There may also be penalties to any violations of the secrecy. Such measures may have an effect in particular in cases where the voter wants to protect the vote. To what degree it also effect the less conscious uncontrolled voting may be much more uncertain.

If and when voting in uncontrolled environment becomes an offer to all voters the role of the schools, election administrators and NGOs in educating new generations in the secrecy of the vote will be of paramount importance. Without the direct illustration provided by voting in a polling station the educational challenge will be tremendous.

4.5 Alternatives to Voting in Uncontrolled Environment

The main reason for introducing postal and Internet voting is to strengthen the participation in elections – either by reversing a negative trend or by even increasing the election turnout. In addition in particular Internet voting has attractive features by providing an immediate and reliable count and the long term costs may be reduced.

Some of these effects may be achieved by introducing the same IT based technology but by making it available only in controlled environment. Voters could be offered extensive possibilities for early voting in controlled environment where the secrecy of the vote is guaranteed. In addition there would be staff available to supervise in the use of the Internet, and even paper ballots may be offered.

For young people such an alternative may still be attractive even though the availability arguably would be less than an Internet service accessible from home.An electronic possibility for controlled early voting would have the same advantages regarding the speed and accuracy of count as regular Internet voting. The costs may be higher, though, since the offer is dependent of staff.

Compared to postal votes electronic voting (both controlled and uncontrolled) would have one big advantage in countries where the time from an election is announced to the election day is short, e.g. in the UK. Electronic voting would reduce the turnaround time now being used for requesting a ballot, printing, distributing ballots and returning them, and the time people can actually cast an early vote would be longer. A controlled electronic early vote may therefore have at least the same effect on turnout as the present postal vote system.

Early voting arrangements even in controlled environment have been criticised by international observer missions to for example Belarus. The basis has been the lack of transparency, pressure on voters to cast an early vote (which 31% of those voting did in the 19 March 2006 elections) and the shortcomings in the records kept from the process[8]. However, early non-controlled voting would represent a much higher risk to the integrity of the vote wherever the election management body does not enjoy full confidence from all parties involved.

5 Conclusions

Voting by mail has become common for groups who would otherwise be disenfranchised. A few countries have adopted postal votes as a choice for any voter. Voting by Internet is implemented in few countries and is being planned by more. Serious security issues and concerns of trust and transparency may be solved, at least in countries where the elections management body is above any doubts regarding their integrity. However, the secrecy of an uncontrolled vote cannot be guaranteed. Even if there is a possibility to regret an uncontrolled vote and vote again in a polling station on election day, the free choice may be only theoretical for groups of voters.

---

[8] See the OSCE/ODIHR statement of preliminary findings issued on 20 March 2006 on the Belarus Presidential elections.

Before Internet voting is opened for the whole electorate governments and inter-governmental organisations should have a thorough discussion about the possible effects of the lack of secrecy of the vote. By the development towards more voting from home the concept of election may change without a real discussion of how that may weaken the voters' consciousness of a secret and personal vote. The lack of protection may not only involve common risks of intimidation and trading of votes, but it may lead to less understanding of the personal aspect of the vote for large groups and young voters may in particular lose out on the educational aspect of a secret, controlled vote.

In this discussion early voting in controlled environment readily available to all voters with the most modern technology may be seen as an attractive alternative. Such alternative may offer the same efficiency and accuracy in the results tabulation, it may offer modern user interfaces, but it will require more people and possibly be more expensive to maintain.

Literature

[NO00] Working Group under the Norwegian Ministry for Local Government: Elektronisk stemmegivning – utfordringer og muligheter. Kommunal- og regiondepartemenet. Oslo 2006. www.dep.no/krd/norsk/dok/andre_dok/rapporter/016051-220023/dok-bn.html.

[UK01] Electoral Commission of the UK: Turnout. How many, who and why? London 2005.

[CE02] Council of Europe. Recommendation adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies. Rec (2004) 11.

[CE03] Council of Europe. Report on the compatibility of remote and electronic voting with the standards of the Council of Europe. Adopted by the Venice Commission at its 58th Plenary Session. Venice 2004.

[OD04] OSCE/ODIHR: Elections Observation Handbook 5th edition. Warsaw 2005.

[KV05] Vollan, K: Observing Electronic Voting. Norwegian Institute for Human Rights. University of Oslo. NORDEM Report No 15/2005. www.humanrights.uio.no/ forskning/publ/publikasjonsliste.html#nr

[KV06] Vollan, K: Zimbabwe: Presidential Elections 2002. Norwegian Institute for Human Rights. University of Oslo. NORDEM Report No 05/2002.

[KV07] Vollan, K: Zimbabwe: Parliamentary Elections March 2005. Norwegian Institute for Human Rights. University of Oslo. NORDEM Report No 11/2005.

[OB08] Oostveen, A-M and P. v. D. Besselaar: Security as Brief. User's perceptions on the security of electronic voting systems. ESF TED Conference on Electronic Voting.

[BI09] Election Court in Birmingham: In the matter of a Local Government Election for the Bordesley Green and Aston Wards of Birmingham City Council Held on 10 June 2004. The Court's judgment. Birmingham 2005.

Coercion-Resistant Electronic Elections with Observer

Jörn Schweisgut

Mathematical Institute
University of Giessen
Arndtstraße 2
D-35392 Giessen, Germany
Joern.Schweisgut@math.uni-giessen.de

Abstract: We introduce an electronic election scheme, that is coercion-resistant, a notion introduced by Juels et al. in [JCJ05]. In our scheme we encrypt the credentials that serve as an authorisation to vote during registration. By using a MIX-cascade we can omit one time-consuming plaintext equivalence test in the tallying. In addition, the observer facilitates registration and voting for the benefit of the voter. Pseudonymisation of the ciphertexts during the voting period implies a permanent secrecy of the submitted votes.

1 Introduction

In 2000 Hirt and Sako [HS00] presented the first electronic voting scheme in which voters were not able to prove their voting decision. This so-called receipt-freeness was achieved under the unrealistic assumption of an untappable channel from each authority to each voter. To solve this problem, Magkos et al. [MBC01] introduced an election scheme in 2001 which is based on a tamper-proof device, a so-called observer. That system has been improved in the following in [Sch06].

Besides the long unsolved problem of receipt-freeness, there are further possibilities for an attack on electronic elections, which were described by Juels et al. in [JCJ05] in 2005. They summed up these attacks by the notion of coercion-resistance and proposed a first coercion-resistant voting scheme. In this paper, an election scheme is presented, which is based on the usage of credentials as a proof of authorisation to vote. The tallying is more efficient than in the scheme by Juels et al. and minimises the voter's effort in the registration and voting phase by employment of an observer.

Even if the encryption was broken the receipt-freeness would be lost but the secrecy of the votes could be guaranteed due to the pseudonymisation, nevertheless.

2 An efficient coercion-resistant observer-based election scheme

For the sake of concreteness, we describe in our paper an electronic voting scheme with a non-malleable ElGamal encryption. The scheme also works with other encryption-systems, e.g. Cramer-Shoup (cp. [CS98]) or Modified-ElGamal (cp. [JCJ05]).

2.1 Setup

The MIX-servers define together a multiplicative group G with prime order $|G|=:q$ and a generator g of G. Then they all generate an ElGamal key pair (s,h) with $h=g^s$ (cp. [Ped91]). Each authority A_j receives a share s_j of s in a (t,n)-threshold secret-sharing-scheme and is publicly committed to this share by $h_j = g^{s_j}$. This key h is published as the public-key of the voting-authorities.

2.2 Registration

Each voter V_i, $(i=1,...,n)$, is informed by the authorities, goes to the registration office and authenticates himself towards the registrars. Then the observer is given to the voter.

The voter chooses a random value $z_V \in_R Z_q$ and computes $h_V = g^{z_V}$ as a public share of z_V. This value h_V is stored on the observer. It is important that the observer itself does not know z_V.

The registrars create a probabilistic encryption $E(\sigma)$ of a random string $\sigma \in_R G$ with the public-key h of the authorities in a distributed threshold manner (cp. [GJKR99]). This ciphertext is transferred to the voter and stored on the voter's observer. The registration authorities re-encrypt $E(\sigma)$ and prove to the voter, that the obtained value $E'(E(\sigma))$ is a correct re-encryption of the transferred ciphertext. In order to prevent the voter from transferring this proof we therefore use a designated-verifier proof (cp. [JSI96]). In addition to $E(\sigma)$ the voter creates a fake credential σ' and encrypts it with the public-key of the voting authorities. This value is also stored on the observer as well as the public-key of the authorities.

At the end of the registration-phase a list $\boldsymbol{V}$ of the voter's credentials is published by the registrars via a robust, verifiable decryption-MIX-cascade of the voting authorities.

2.3 Voting

The votes are decrypted by the MIX-cascade in the tallying and published as plaintexts. Therefore, we can choose a representation of the candidates that enables us to simply tally the votes by adding the values. The candidates are described in a number system with the number of candidates n_L as its basis. Let be $\boldsymbol{L} = (m_1,\ldots,m_{n_L}) = (1, n_L, n_L^2,\ldots,n_L^{n_L-1})$ the set of candidates.

Each voter chooses random numbers $a,a' \in_R Z_q$ and encrypts his candidate choice m out of $\boldsymbol{L}$: $(x,y)=(g^a,h^a m)$. Furthermore, he computes $g^{a'}$. These values are sent to the observer which chooses random values $b,b' \in_R Z_q$ and re-encrypts the ciphertext:

$$(x',y')=(g^b g^a, h^b h^a m).$$

In addition to this, the observer re-encrypts the stored ciphertext $E(\sigma)$ of the credential with the public-key of the authorities and obtains $E''(E(\sigma))$. It calculates $g^{a'+b'}$ and the necessary value for the non-malleability

$$b \cdot H(g,x',y',g^{a'+b'},E''(E(\sigma)))+b'.$$

The cryptographic hash-function H serves as a challenge in the non-interactive zero-knowledge proof of non-malleability.

The observer sends

$$(x',y',g^{a'+b'},b \cdot H(g,x',y',g^{a'+b'},E''(E(\sigma)))+b',E''(E(\sigma)))$$

to the voter.

If the observer works correctly the voter can compute (g^b,h^b) from it. Then the voter can complete the non-interactive zero-knowledge-proof of non-malleability and independent vote-creation respectively:

$$(a+b)H(g,x',y',g^{a'+b'},E''(E(\sigma)))+(a'+b').$$

Without any knowledge of the used values a and b it is impossible to create this message (cp. [TY98]).

In order not to stress the measure of confidence in the observer, the observer proves correct encryption in a designated-verifier proof to the voter.

The voter has to prove publicly, that he has encrypted a valid candidate choice. This can be done e.g. by a non-interactive witness-indistinguishable proof P (cp. [CDS94]). If not, he could cast any message as a vote, which would not be tallied, but its value could be used as a receipt towards a coercer. This does not mean that the voter cannot void his vote. It is possible that one option on the candidate list is "cancel vote".

Then the encrypted non-malleable ElGamal message together with the encrypted credential as an authorisation and the proof P is:

$$E(m)=(x',y',g^{a'+b'},(a+b)H(g,x',y',g^{a'+b'},E''(E(\sigma)))+(a'+b'),E''(E(\sigma)),P).$$

The voter sends all this to the electronic bulletin board, a publicly readable memory to which everyone can append but not erase or alter data.

Therefore, the zero-knowledge proof of non-malleability and the proof of a correct candidate choice are publicly verifiable.

The messages from the voters to the bulletin board have to be sent via an anonymous channel. Such a channel can be achieved by employment of a MIX-cascade. To guarantee a permanent secrecy of the votes, the messages from the voters have to be secured by enabling voters to cast ballots in public places or from any point of the net. Thereby, the votes are mixed with other ones even if the encryption and thus the anonymity of the MIX-cascade is broken.

2.4 Tallying

Votes without a valid zero-knowledge proof of non-malleability or without a valid proof *P* are ignored. According to a predetermined policy, the votes are ignored that have been cast together with equal credentials, i.e. equivalent credential ciphertexts. That means that at most one vote per credential will be tallied. To decide whether two ciphertexts are encryptions of the same underlying credential, a pairwise plaintext equivalence test (cp. [JJ00]) is used. Afterwards the votes pass the verifiable robust decryption-MIX-cascade. Thereby, the parts of the message that include the credential and the vote are not separately but synchronously permutated. The output of the MIX-cascade is a randomly permutated list of pairs, each pair consisting of a plaintext-vote and a credential. The credentials are compared with the list *V* of authorised credentials. Votes without valid credentials are deleted. The remaining votes are publicly tallied.

3 Criteria and Analysis

Up to now there have been no common criteria for democratic electronic elections. But it would be wise if the electronic elections fulfil at least the requirements that are set on conventional secret ballot elections. In addition there are some further requirements that derive from the media (e.g. correctness, verifiability, non-malleability and coercion-resistance).

The described voting scheme fulfils all the demands that are put up for traditional secret ballot election and to a great extend the requirements that have been set up for electronic voting schemes so far.

3.1 Authorization, Unforgeability, Single vote

The verification of the authorization and the unforgeability of votes are guaranteed by comparing the credentials with the list of valid credentials. After the registration the valid credentials are anonymised and published via a verifiable MIX-cascade. With this list, everybody can check if a message comes from an authorized voter, but it is impossible to find out from which one. Unauthorized messages are ignored.

The unforgeability of votes is based on the security of the scheme used to encrypt the credentials. Such public-key encryptions are not indefinitely secure. On the other hand one does not need a perfect secure encryption (i.e. a one-time-pad) as a break of the scheme is only advantageous for an adversary in the period before the actual tallying.

If only the first cast votes with correct credentials are considered for the tallying and later submitted votes of the same voter are declared invalid and are erased, then it is guaranteed that one voter can only cast one valid vote.

3.2 Verifiability

As the bulletin board is publicly readable, everybody can prove the non-malleability (independent vote-creation) and that the votes contain valid elements of the candidate list. The plaintext-equivalence-tests for the encrypted credentials to prevent double-voting are also publicly verifiable. During the tallying the votes are sent through a MIX-cascade and decrypted. So the actual tallying can be done by everyone. This means that the verifiability of the voting schemes derives directly from the verifiability of the MIX-cascade.

3.3 Correctness

The correctness of the tallying is guaranteed if all voters are able to cast the vote of their choice, i.e. all voters can understand and check the encryption of the observer. This is ensured by the designated-verifier- and the witness-indistinguishable-proof, the verifiability of the MIX-cascade and the public tallying of the plaintext votes.

3.4 Honesty, Robustness

A dishonest voter is not able to submit an invalid vote that is accepted and tallied. On the one hand he has to include a proof, that the cast vote contains a valid candidate choice. On the other hand the votes are decrypted and invalid votes will be ignored.

It is due to the verification of each action of each MIX-Server that fraudulent authorities can be identified and excluded. As long as there are not more than a certain threshold of dishonest MIX-servers the election can be completed without them. Therefore the voting scheme is robust.

3.5 Expenses

The complexity of communication depends on the used proofs, i.e. the designated-verifier proof, the zero-knowledge-proof of non-malleability and the witness-indistinguishable-proof of the valid choice. These proofs can be efficiently implemented and the communication costs are independent of the number of authorities as well as of the number of candidate choices.

The registration can be done for several elections. The efforts on the side of the voters are acceptable.

3.6 Anonymity

The anonymity of each voter is guaranteed if the used credential cannot be traced back to the voter. That is the case in this voting scheme, as the votes are cast via an anonymous channel (MIX-cascade) *and* the voters can cast their votes from any point of the net. It is impossible to find out which choice a voter has made, even whether a specific voter has cast a vote.

Only those who know the credential of a voter prior to the tallying may find out *if* a voter has submitted his message. Assuming that the used encryption would be broken anytime after the tallying, then the credentials and the anonymous channel still conceal the relation between the votes and the voters - as long as the voter has not given his correct credential away prior to the tallying.

3.7 Independent vote-creation

It is impossible to copy a vote of another voter, because he has to prove in zero-knowledge that he knows the randomness used to encrypt the vote. Due to the non-malleability (i.e. chosen-ciphertext-security) of the encryption, it is impossible for an adversary to cast a vote that bears a known relation to a vote of another voter.

3.8 Coercion-resistance

The voting scheme is receipt-free, i.e. it is impossible that a voter creates a receipt which indicates his choice. If he was able to create one, he would be coercible or corruptible. It is even thinkable that the voter is controlled by an adversary and casts the vote the adversary wants him to. As long as he uses a fake credential, this vote will not be tallied and the voter can still cast his vote he wants to. In addition to that, the scheme is secure against a randomization attack as it is possible in [HS00], because only *one* candidate choice has to be encrypted to construct and cast a vote. It is not even noticeable if a voter has cast a vote and that is why it is impossible to force a voter to abstain from the election. Therefore the scheme is coercion-resistant.

4 Conclusion

The electronic voting scheme fulfils the requirements set on democratic electronic elections in section 3 including coercion-resistance.

If the encryption-key of the authorities was compromised, the pseudonymisation would guarantee the secrecy of the votes, unless the voter publishes his pseudonym before the actual tallying takes place.

The observer does not fulfil the "classical" tasks of an observer (cp. [CP92] and [CP93]) but it rather serves as a convenient and secure transport.

If an adversary forces a voter to hand over his observer, then the voter can give him a wrong PIN. That results in the fact that the observer uses the fake-credential. The voter is able to vote without observer even if the adversary has tried to vote with his observer before.

By using the encryption of credentials and the MIX-cascade for the generation of the list of authorised credentials, we can omit one of the time-consuming plaintext-equivalence tests during the tallying.

Only the plaintext-credentials have to be compared.

References

[CDS94] Ronald Cramer, Ivan Damgård and Berry Schoenmakers: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In Yvo Desmedt, editor, *CRYPTO '94*, LNCS 839, pages 174-187. Springer, 1994.

[CP92] David Chaum and Torben P. Pedersen: Wallet Databases with Observers: In *CRYPTO '92*, LNCS 740, pages 89-105. Springer, 1992.

[CP93] Ronald Cramer and Torben P. Pedersen: Improved Privacy in Wallets with Observers (Extended Abstract): In *EUROCRYPT '93*, LNCS 765, pages 329-343. Springer, 1993.

[CS98] Ronald Cramer and Victor Shoup: A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack: In Hugo Krawczyk, editor, *CRYPTO '98*, volume 1462 of *LNCS 1462*, pages 13-25. Springer, 1998.

[GJKR99] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin: Secure Distributed Key Generation for Discrete-Log Based Cryptosystems: In *EUROCRYPT '99*, pages 295-310, 1999.

[HS00] Martin Hirt and Kazue Sako: Efficient Receipt-Free Voting Based on Homomorphic Encryption: In *EUROCRYPT '00*, LNCS 1807, pages 539-556. Springer, 2000.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson: Coercion-Resistant Electronic Elections: In *WPES '05*. ACM CCS, November 2005.

[JJ00] Markus Jakobsson and Ari Juels: Mix and Match: Secure Function Evaluation via Ciphertexts: In Tatsuaki Okamoto, editor, *ASIACRYPT '00*, LNCS 1976, pages 162-177. Springer, 2000.

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo: Designated Verifier Proofs and Their Applications: In *EUROCRYPT '96*, LNCS 1070, pages 143-154. Springer, 1996.

[MBC01] Emmanouil Magkos, Mike Burmester, and Vassilios Chrissikopoulos: Receipt-Freeness in Large-Scale Elections without Untappable Channels: In *I3E '01*, IFIP Conference Proceedings 202, pages 683-694. Kluwer, 2001.

[Ped91] Torben P. Pedersen: Non-interactive and information-theoretic secure veriable secret sharing: In *CRYPTO '91*, pages 129-140, 1991.

[Sch06] Jörn Schweisgut: Effiziente elektronische Wahlen mit Observer: In *GI - Sicherheit 2006*, LNI Proceedings P-77. Gesellschaft für Informatik e.V. (GI), February 2006.

[TY98] Yiannis Tsiounis and Moti Yung: On the Security of ElGamal Based Encryption: In *PKC '98*, LNCS 1431, pages 117-134. Springer, 1998.

Session 7: Implementing E-Voting

Maintaining Democratic Values in e-Voting with eVACS®

Carol Boughton

Software Improvements
Unit 20, 16 National Circuit
2600, Barton ACT, Australia
carol@softimp.com.au

Abstract: The principles of equality, secrecy, security and transparency apply to any democratic election system irrespective of whether paper ballots, mechanical or electronic means are used to conduct the election. All these principles were mandated as requirements, designed into, and successfully operated as features of, eVACS®, the electronic voting and counting system used since 2001 by the Australian Capital Territory Electoral Commission. How eVACS® achieves these requirements is described in this paper, with particular emphasis being given to security and transparency and the approaches adopted to ensure verifiability via electronic audit trails.

1 Introduction

All democratic election systems have many features in common no matter where a particular system is applied.

In the UK [Wa02], six principles were initially identified as forming the minimum requirements of a democratic election procedure. Public consultations established wide community support as well as leading to their simplification to three principles.

1. the **doorkeeper** principle: - Each person desirous of voting must be personally and positively identified as an eligible voter and permitted to complete no more than the correct number of ballot papers.

2. the **secrecy** principle**: -** Admitted voters must be permitted to vote in secret.

3. the **verification, tally and audit** principle: - There must be some mechanism to ensure that valid votes, and only valid votes, are received and counted. The system must be sufficiently open and transparent to allow scrutiny of the votes and subsequently the working of the political process.

More recently three democratic values were identified as being essential to any voting system adopted in the USA [To04]:

i) **equality** (of political participation), including racial equality; multi-lingual access; disability access; inter-jurisdictional access (or no differential treatment to voters based on the county or jurisdiction where they reside);

ii) **security** (the resistance of votes and vote totals to fraud and other forms of manipulation); and

iii) **transparency** (the capacity to produce auditable results in which both candidates and voters can justifiably have confidence).

These values or principles of **equality**, **secrecy**, **security** and **transparency**, apply to any democratic election system – no matter whether the election is conducted using paper ballots, mechanical or electronic means. Exactly these requirements were recognised and specified in 2000 for the electronic voting and counting system eVACS®, successfully used by the Australian Capital Territory (ACT) Electoral Commission in the 2001 and subsequent ACT Legislative Assembly elections [El02] [El05]. Descriptions follow on how eVACS® ensures **equality, secrecy, security** and **transparency** with particular emphasis on the approaches adopted to ensure verifiability via eletronic audit trails.

2 Equality

The voting set-up is identical for all users. For the vision impaired, or voters with poor reading skills, audio is provided and, if required, a larger screen. Privacy is maintained by the use of a headset, with voters able to use their own headset or a disposable one. The use of a (special) keypad to record choices/preferences enables voters with a range of physical impairments to vote without assistance. For preferential or proportional election systems in which voters are required to indicate a sequence of numbered preferences, selection of a candidate automatically assigns the next number in the sequence ensuring there are no missing or repeated numbers. Thereby ensuring voters do not unintentionally vote informally.

Other features addressing equality include instructions being provided in the voter's language of choice, as well as the local language of the region, using any alphabet or character set. If permissible by law, voters are able to vote away from their normal polling place. The hardware can be placed to give voters their choice to either sit or stand to vote.

3 Secrecy

Vote secrecy is maintained in five ways. First, the voting screen is positioned so that no other person is able to see a constructed vote. Second, the system fits in a normal (cardboard) voting booth. Third, for the standard arrangement no noise signals are emitted to alert anyone else as to how a voter may be voting.

Fourth, because voters 'navigate the electronic ballot' using the keypad, it is extremely difficult for anyone else to be able to discern who is being voted for. And fifth. a voter can 'hide their vote' if they need to seek assistance from an official.

In addition, all of the equality features (described in Chapter 2) increase the number of people who can vote without assistance, and thereby vote in secret.

4 Security

Security involves a number of design and operational aspects covering software and hardware, including a log of all activities. Automated set-up arrangements ensure that an election is run from a series of auditable write once CDs, and on loading the software, the hard disk/s are reformatted thereby removing any existing operating system and other software. Limited functionality, for voters and officials, means software cannot be modified during an election.

At the polling place each voter is randomly assigned a barcode, from a restricted set of barcodes internally generated by the system. The barcode determines in which election/s a voter is eligible to vote, ensures only completed votes are stored, and identifies incomplete votes if the network is disrupted. Whether a barcode has been used is checked automatically before voting commences and may also be checked manually.

All votes are cast in a public polling place over an isolated LAN with votes only stored on physically secure voting servers. No votes are stored on voting machines used by voters. The votes are stored simultaneouslyin two separate databases to guard against loss of votes due to hardware failure. Additionally, the outcome of a rerun in sequential order of voter keystrokes must match with the voter's choices before a vote is recorded and stored. Downloading of votes at the end of polling requires password and encryption keys, not transmitted to polling place officials until after polling closes. Votes are encrypted and downloaded to two write once CDs with checksum. Both disks have to be loaded into the counting server and match the checksum.

The combined auditing and internal security features ensure a court is able to verify the CDs that were used for a specific election, and that the election result is accurate and has not been tampered with in any way.

4.1 Security of hardware

The election software runs on any hardware that supports the Linux operating system. The degree of in-built security of hardware can vary significantly between equipment. Consequently, there is an emphasis on maximising security via the software with physical security an added feature where available.

Used in the 2004 ACT Legislative Assembly Election, the ROC - Rugged Operations Computer - specially designed for electronic voting [Ro04] [El05], provides advantages over standard PCs in respect of ease of set-up and use, as well as better protection against external damage from liquids, solids, heat and physical damage. Each polling place LAN network is also physically protected against attempts to break into the system.

5 Transparency

In paper based voting systems transparency is managed by having observers/scrutineers present at different stages of the voting and counting processes, such as: empty ballot box and then securing (eg by sealing or locking) the box at the start of polling; ballot boxes remaining secured until after close of poll; only those people who actually attend the polling place are marked off the electoral roll at that polling place; assistance to voters incapable of marking their ballot paper by themselves; only voters place the appropriate ballot papers in the ballot box during polling; emptying of ballot box at the close of polling; counting of ballot papers after close of poll; secure transportation and/or storage of the votes; and recounting of votes.

Electronic voting and counting must, by necessity, change the nature of scrutineering, but computerising the voting and counting processes ought not prevent elections from being transparent, nor prevent scrutineers from observing all aspects of the voting and counting processes. "*A computerised voting and/or counting system is in essence a series of mechanical steps, facilitated by computer hardware and computer programs. A thorough understanding of the way in which the hardware and programs work – the electronic trail – should serve to demonstrate that the system is transparent, and in particular, that 'what goes in is what comes out'*." [Gr03]

There are some activities of scrutineering that are outside the scope of electronic voting. To ensure the anonymity of votes there can be no connection between the voter's details and their vote. Any system for marking people off the electoral roll (either paper or electronic) must be independent of the voting and counting processes. Hence, the observation process to ensure only eligible people vote continues independently of eVACS®.

As with paper ballots, transparency in an electronic election has a number of stages, grouped into five levels, none of which is sufficient by itself to demonstrate the required transparency for an election. Each level of transparency must be completely fulfilled.

In the first level of transparency code is available so others can assure themselves that the software does what it is meant to do and nothing else. The Electoral Commission arranged for independent auditing of the software code used for acceptance testing and then in an election. The audited code was released publicly.

After the 2001 election, researchers from the Australian National University independently verified the counting algorithm and replicated the results of the 2001 ACT Assembly election.

The second level of transparency requires the correct operation of the vote recording and paper ballot data entry processes, and votes counted accurately according to the specified election system. Extensive testing prior to the software being put into service was undertaken, plus acceptance testing by the customer prior to auditing with representatives from political parties and disability groups observing.

For the third level of transparency, the software used for an election can be shown to be exactly the same software that passed first and second levels.

The fourth level of transparency involves Officials demonstrating the in-built features of the closed system ensure the limited functionality cannot be tampered with during use in an election, there is an empty electronic ballot box at start of election, the number of votes (formal/informal) in electronic ballot box, the initial results (for specific polling places), and secure downloading of votes. Downloading of votes is security controlled both to download and when uploading into counting server with encryption of votes, password access and checksums on CDs.

To achieve the fifth level of transparency voters and officials have to be confident that none of the recorded votes are lost, and that only completed votes are recorded. Activities to meet other levels demonstrate the former, while the barcode provided to each voter is used to start and end a voting session and ensure only completed votes are recorded.

In addition, there must be a well-documented 'electronic trail' with all the development artefacts and code available for independent auditing, and the source code published for examination by interested persons.

On the introduction of computer technology as applied to electoral matters in Australia, the then Commonwealth electoral authority's explanation for its reluctance to move too rapidly into computers in 1982 was: *It is absolutely essential not only that an election system be fair, but that it is seen to be fair. The safeguards built into the current system are the product of many years of experience. The full-scale introduction of a new, and much more complicated system could create opportunities for illicit interference, or allegations of such interference, with the electoral process. A completely new security process would have to be developed – one which would be acceptable to the electorate, the candidates and the political parties. (op cit Hansard V.129 1982 1614).* [Mc01]

While new steps in computerisation of the election process have subsequently been taken each year, they have not been submitted, step by step, to parties and candidates for open debate, let alone to the electorate *(page 166 of [Mc01]).*

In Ireland the Commission on Electronic Voting in its first report [Ir04] was unable to recommend use of the chosen electronic voting system because the accuracy and security could not be established as: i) there was not sufficient time to fully test the system, ii) the full source code had not been made available, iii) the version to be used was unknown and therefore the accuracy of the system could not be certified, and there were concerns that secrecy of the vote might be compromised.

In marked contrast, the development and introduction of electronic voting and counting in the Australian Capital Territory occurred with public participation. eVACS® was developed after direct public consultation had led to legislative changes to enable electronic voting and counting, undertaken in association with a Reference Group (with representatives of candidates, political parties and the public) whose members were able to participate in the acceptance testing, and the source code released for public scrutiny before use in an election.

Apart from ensuring a completely transparent electronic trail, elimination of opportunities to tamper with election results is another benefit of electronic voting. Opportunities such as ballot box stuffing, completed ballot papers from a polling place being "lost" and completed ballot papers deliberately inserted in the wrong stack for counting.

Electronic votes cannot be prepared in advance; voting must occur at the polling place and under the direct observation of others. The period when electronic voting is available at any polling place is logged by recording the time whenever the system is activated (start voting) or deactivated (stop voting). A unique barcode must be obtained for each electronic vote.

Electronic votes are stored in duplicate on the voting server at a polling place. The votes are downloaded twice onto separate write once CD-ROMs with a checksum. Details from both CDs are loaded into the counting server and confirmed with the checksum before the votes are added to the counting database. The only option for downloading votes is to download all votes stored on the voting server. Votes for a particular polling place can only be added once to the counting database. A report is available of polling places from which votes have not been imported into the counting database.

Once confirmed by a voter, the limitation of functionality means there is no way to interfere with the content of an electronic vote. There is no means to change the counting program once a specific election has been set-up.

5.1 Recounts and petitions

Recounts were introduced to address the known failings with manual counting of votes, and usually occur when the result of an election is very close. Either the electoral agency or a candidate may seek to have the votes recounted. Also, in some jurisdictions there is a mandatory requirement to recount a proportion of all votes to check the accuracy of the manual count. Whereas in other jurisdictions, a candidate, a voter or the electoral agency may dispute the validity of an election via a petition to a court.

Electronic voting and counting has significant impact on the conduct of recounts and for contesting election outcomes in the courts. The demonstrable accuracy of electronic voting and counting avoids the unnecessary recounts when election results are close. Mandated recounts are not practical with electronic voting, although a random set of votes could be printed and counted manually with less accuracy. With petitions, the issues are not ones of 'who did or did not do what' or 'what was permissible under the election legislation' but whether the computer program used met the appropriate standard of accuracy, reliability and trust. The transparency has to enable a court to independently establish the accuracy, reliability and trust in the election system.

5.2 Electronic voting and voter verifiable audit trails

There is no question about the need for voter verifiable audit trails with electronic voting. However, as per [To04], a 'voter verifiable audit trail' is not synonymous with '*paper* ballot replicas'.

Voter verifiable *paper* audit trails are often cited as the solution to addressing problems encountered with electronic voting in the USA. Yet as has been shown [To04] [El05], whether a voter verifiable paper audit trail is both a practical solution and an effective means of preventing fraud is highly questionable. For example, the tape for a voter verifiable paper audit trail system used in Clark County, Nevada, USA, contain 64 voter verifiable paper ballots from one voting machine, is a strip of 10cm (four inch) wide paper, just under 120 metres in length (318 feet) and "it took a four person team - one counting votes, one verifying and checking for errors and two recording results – about four hours to check one tape, or nearly four minutes per ballot" (photograph in [eo05]). The ability of election officials to accurately determine election results under such circumstances becomes a costly exercise in checking and cross checking.

The USA is not the only country where concerns have been raised about the electronic voting system used. Others are Brazil [Re03] and the NEDAP Powervote system trialled in Ireland [Ir04].

There are some who believe no electronic voting system can be trusted and therefore a paper audit trail is absolutely essential [Me01]. Yet others caution against sacrificing the voting rights of disabled voters and non-English speaking citizens in order to achieve the admirable goal of enhancing election security and transparency [To04]. A voter verifiable paper audit trail is obviously not an option for the vision impaired, poor readers, or voters who cannot read the language of the print out.

Not all the issues raised with electronic voting have been about ensuring votes are recorded accurately at the polling place. There have been reports of vote databases being accessed by the public, uncertified software being used, bug fixing occurring during an election, and equipment being certified without meeting certification requirements [Bl05]. With an appropriate 'voter verifiable audit trail' none of these issues should eventuate.

All of the concerns with electronic voting have arisen where there has been no transparency of the software used nor any serious attention to security issues prior to implementation of the system. In contrast, with eVACS® all of these issues were addressed before the system could be used in an election.

6 Voting is not everything

Maintaining democratic values does not simply apply just to the voting process. The third principle (see Chapter 1 and [Wa02] and [To04]) is to ensure that only valid votes are counted and that the counting process is auditable and transparent. Incorporation of this requirement starts with the set-up for a particular election, and applies equally to all other phases of the election process.

One of the major benefits of electronic elections is the speed at which election results can be determined. To achieve these benefits though, all votes need to be available electronically. Wherever postal voting or the equivalent is available not all votes will be recorded electronically, so there is need for a module that will convert paper votes into electronic votes. Ensuring the same level of accuracy and trust, as for electronic voting, in this conversion process is absolutely critical to ensuring only valid votes are counted.

Having a fully auditable process throughout all phases of an election therefore means that features of transparency and security have been applied to all modules of the eVACS® system, as well as to the interconnections.

6.1 Set-up election

Reference is made in Section 4 to an election being run from a set of auditable write once CDs, and to limited functionality such that the software cannot be modified during an election. In practical terms, the auditable set-up election CD is loaded on to a standalone PC – the set-up election server, and the hard disk reformatted. The set-up election server is then used to generate the voting server and data entry/counting server CDs for a specific election. All CDs are treated with the same degree of protection as ballot papers when being transported but in addition have in-built checksum and encryption features to ensure what was downloaded from one part of the system is identical with what is loaded into another part of the system.

eVACS® is referred to as a ‘closed system’ since there is no interaction with any other software.

6.2 Entry of non-electronic votes

The original eVACS® uses a data entry process for incorporation of non-electronic votes with double entry of the paper ballot details and separate authorisation for editing when entries do not match. Scrutineers are able to observe the entire process.

Developments in scanner technology since 2001 mean there may be an alternative to data entry for managing non-electronic votes, but with two issues that need to be addressed. First, scanning of all paper ballots is not always achievable, and second, particularly when preference numbers are written, not every paper ballot can be scanned with 100% accuracy. As a consequence an auditable and traceable editing process equivalent to that provided for data entry in eVACS® is necessary to ensure that only valid votes are entered and counted.

6.3 Counting and reporting

Counting has different facets that must all be proven to be auditable and transparent: the actual counting algorithm; the process by which electronic votes from different sources are merged for counting; and the actual reporting of results.

Counting algorithms don't just count votes. They determine which votes are valid (or formal) votes. Also, they may need to cater for different interpretations of vote information from votes received by a candidate who dies before the election results are announced. Additionally, when two or more candidates receive the same number of votes there may be a formal separation process that needs to be initiated during the counting process.

For many elections, votes from a number of sources such as different polling places, or electronic and non-electronic votes need to be merged for counting. Ensuring that votes can only be included once is critical to undertaking an accurate count.

Another, often overlooked aspect is the potential for manipulation of results after a count has been undertaken. It is important that the results are not accessible before printing the official election results.

7 A final comment

As with any new development, lessons are learnt from use. In the reviews of each of the 2001 and 2004 elections, enhancements were recommended [El02] [El05] and agreed by the ACT Government [El03]. What is significant about these enhancements is that none sought to change the basic equity, secrecy, security and transparency features designed into the system.

The 2001 recommendation to improve 'the set-up process to automate the loading of election details, particularly candidate names and sound files' was implemented by establishing the set-up election module which turned eVACS® into a 'closed system', thereby further enhancing security.

References

[Bl05] The Official Blackbox Voting Website http://www.blackboxvoting.org/

[eo05] electionline.org "*Recounts: From Punch Cards to Paper Trails"*, 2005 http://www.electionline.org/Portals/1/Publications/ERIPBrief12_FINAL.pdf

[El02] Elections ACT, "*The 2001 ACT Legislative Assembly Electronic Voting and Counting System Review*" ACT Electoral Commission, 2002 at http://www.elections.act.gov.au/Elecvote.html

[El03] Government response to the 2001 ACT Legislative Assembly Electronic Voting and Counting System Review http://www.elections.act.gov.au/EvoteRG.html

[El05] Elections ACT, "*2004 ACT Legislative Assembly Electronic Voting and Counting System Review*" ACT Electoral Commission, 2005 at http://www.elections.act.gov.au/Elecvote.html

[Gr03] Green, Phillip Chapter on "*Transparency and Elections in Australia: The Role of Scrutineers in the Australian Electoral Process"*, in *Realising Democracy: Electoral Law in Australia*, G. Orr, B. Mercurio and G Williams (eds), The Federation Press, 2003, pages 226-228.

[Ir04] Ireland Commission on Electronic Voting First Report on *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System,* 2004 http://www.cev.ie/htm/report/first_report/pdf/00Index.pdf

[Mc01] McGrath, Amy "*The Frauding of Votes*" with an Introduction by Bob Bottom, Tower Books Wholesale, ISBN 0-9587104-3-0, 2004.

[Me01] Mercuri, Rebecca, *Rebecca Mercuri's Statement of Electronic Voting* http://www.notablesoftware.com/RMstatement.html, 2001

[To04] Tokaji, Daniel P: *The Paperless Chase: Electronic Voting and Democratic Values.* Ohio State Public Law Working Paper No. 25, 2004 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=594444

[Re03] Rezende, Pedro AD:*Electronic Voting Systems - Is Brazil ahead of its time?* Paper prepared for the First Workshop on Voter-Verifiable Election Systems Denver, USA, 2003 http://www.cic.unb.br/docentes/pedro/trabs/election.htm

[Ro04] Rugged Operations Computer http://www.roc-solid.com/

[Wa02] Watt, Bob: *Implementing electronic voting in the UK: The legal issues* Office of UK Deputy Prime Minister http://www.odpm.gov.uk/index.asp?id=1133606

Transition to electronic voting and citizen participation

Letizia Caporusso, Carlo Buzzi, Giolo Fele, Pierangelo Peri, Francesca Sartori

Dipartimento di Sociologia e Ricerca Sociale
Università degli Studi di Trento
V. Verdi, 26
38100 Trento, ITALY
provote@soc.unitn.it

Abstract: This paper draws attention to the need of a systematic socio-technical approach to introducing electronic voting and presents early results from a pilot project conducted by the Provincia Autonoma di Trento, Italy. Main features of this experience are the constant monitoring of the social impact and the development of a technological solution in accordance to the suggestions provided by the users themselves. We recommend that no sudden switch to a new form of ballot should be imposed on electors but rather that research is to be fostered in order to uncover and preserve the traditional and symbolic connotations embedded in the act of voting.

1 Introduction

At the time being, the Italian ballot system consists of a paper-and-pencil method and electors are allowed to vote only in the section where they are registered. The vote is expressed by drawing a cross on the symbol of the party and by – eventually – writing down the names of the candidates. During the count contentions do arise, among other reasons, due to the misinterpretation of ballots that are not clearly written or ballots that seem to have been purposely marked in order to be recognized. Citizens who are physically impaired have their vote cast by a person they trust, as no technological support is available to help them vote on their own.

In order to overcome these obstacles as well as to keep the democratic process aligned with the development of e-society, new forms of voting are being considered by the Provincia di Trento which, because of historical and political reasons, benefits from special autonomy status in respect to other Italian areas and can determine by its own legislation how the Council and the President of the province are elected. Such a peculiar condition is favouring a boost in the development of e-government, including a thorough study of the possibility to introduce e-vote for local elections: this project, named ProVotE, was set up since December 2004 and aims at crafting a voting machine that, complying with the standards indicated by the Venice Commission [Ve04], is accepted and easily employable by electors regardless of their age, sex, education and confidence in the use of technology.

2 A systematic approach

ProVotE is characterized by an on-going round-table[1] where representatives of the Provincial Electoral Bureau, researchers from the Centre for Scientific and Technological Research (IRST) and from the Department of Sociology and Social Research of the Università di Trento meet on a regular basis to share developments in each area of expertise and plan systemic activities aimed at testing electors' reactions to a likely, but yet to establish, switch from paper-and-pencil to electronic voting. In the light of the key role played by the study of the social impact, we designed a set of investigations spread over one year in order to get the clearest picture of citizens' beliefs and attitudes toward e-voting before and after the two field tests that took place in May and November 2005.

We define social impact as any change occurring in the symbolic order or in the concrete behaviour of a population in consequence of the exposure to an external stimulus. In investigating the social impact of the introduction of electronic voting we had to consider people's attitudes, expectations, fears and practices *before* they even heard of the possibility of e-voting in their own area, *during* the field tests and some time *after* these trials. The research plan included:

- 8 preliminary focus groups to explore practices and habits related to voting;
- over 2500 telephone interviews to uncover attitudes toward electronic voting and assess the technological ability of the population;
- 160 supervised trials aimed at investigating man-machine interaction by means of both questionnaires and ethnographic observation;
- monitoring of turnout to open trials held in the towns chosen for the first field test;
- a large scale field test in five towns alongside local elections – involving 6950 participants – and a smaller scale follow-up field test with 336 electronic voters;
- analysis of electoral data and comparison of electronic and paper-and-pencil results;
- 1200 telephone interviews four months after the tests to compare attitudes and motivations of those who tried electronic voting and those who did not.

This paper offers a brief account of the main empirical results of the research activities summarised above and underlines the importance of integrating the technological with a sociological perspective, which considers the feedback provided by the end users of electronic voting systems.

[1] The authors acknowledge the support received by the Provincia Autonoma di Trento, especially by the Director of the Electoral Bureau, Patrizia Gentile. We wish to thank Adolfo Villafiorita (IRST) who coordinated the technological team and Giorgia Fasanelli (CRC Trentino).
As with any large project the results presented in this paper are based on the joint work of several people: Andrea Cossu, Lodovica Simionato, Elisa Fanelli analysed qualitative data; Enzo Loner, Cristina Margheri, Michela Frontini analysed surveys.

3 Transition to electronic voting and citizen participation

3.1 The sense of voting and the practices related to elections

The socio-anthropological literature describes the activities associated with elections as *rituals* which enhance the sense of belonging to a civic community [Ed64; Ke88]. Little has been said, however, about the intrinsic value and significance of the act of voting from a subjective standpoint: the *sense* of "having one's say", as well as the *body of practices* related to the expression of the citizens' will, appears to have been widely neglected. A preliminary "qualitative" study was therefore aimed at unveiling the entangled mixture of symbolic and material elements that come into play in the apparently ordinary act of casting a vote.

The focus groups portrayed a rather customary and standardized schedule of the day of elections: people show preferences about the time of day devoted to voting (i.e: early in the morning or late at night to fit with Sunday outings, rather than just before or just after Holy Mass); which might result in queues and a potential intolerance towards any innovation, should it imply a longer time to mark the ballots. The habit of going to vote together with relatives also appears to be rather widespread, in the main if going to the polling station requires a means of transport: the presence of younger people in family groups going together to cast their ballots might then be crucial to reinforce institutional tuition and to bridge the technological gap between generations, should electronic voting be extensively introduced.

More considerations pertain electors' awareness of their ability to vote "properly": whereas paper ballot is considered an easy, automatic act in which the chance of making mistakes is minimal, the idea of voting electronically evokes more perplexities. The perceived social impact can be summarised in the following key issues, which need to be taken into careful consideration, as beliefs often anticipate or even modify the course of future events:

a. interviewees believe that e-voting will have no effect in increasing the turn-out
b. interviewees fear that costs for elections will increase, compared to paper ballots
c. interviewees project their worries onto a specific segment of population (senior citizens) and fear that this social group might be, though indirectly, deprived of the right to vote
d. interviewees reckon age will impact more than educational capital or technological ability
e. a general distrust in politics and a feeling of uselessness of one's vote are often expressed, which, according to the interviewees, might result in an apathetic or critical attitude toward innovations in such a delicate matter.

Nonetheless, the informants (especially the youngest) also brought evidence of some hindrance experienced in the choice of candidates with the paper-and-pencil method: this requires to write down the names properly and correctly to avoid having the vote invalidated, which gives rise to frequent undervoting.

Some practices related to paper voting emerged, such as the frequent use of facsimiles, which are mailed by candidates and show how to fill in the ballot. In the light of such a habit, keeping the visual layout of the touchscreen consistent to that reproduced on paper does not require a major change in the electors' expectations and is welcomed by all interviewees.

A surprising result of this preliminary investigation relates to the citizens' opinion about the use of a printer that allows electors to verify their ballot [e.g. Me02]: unexpectedly, they seem to consider it an unnecessary token which does not fit with the idea they have of "electronic" voting. They argue that the cost of printing and counting ballot proofs will equal or exceed the expense of traditional ballots without suggesting the same feeling of control and trust that the paper offers.

At the same time it is important to stress that the confidence of electors in the traditional procedure is also influenced by the fact that anyone has the chance to be a scrutinizer or a list representative and therefore to be protagonist and witness of the entire process: the switch from material to "immaterial" practices seems to deprive the community of the direct contact with the ballots.

By interviewing the scrutinizers, further evidence related to the need of trust also emerged:

a. trusting that one's ballot is personal and secret (thus guaranteeing one's freedom of choice)
b. trusting that each and every vote is actually counted (i.e., not "thrown away")
c. trusting that the ballot count truly respects the voter's will (also by being available for further controls and re-counts)

The board of scrutinizers appears to be a peculiar kind of organization, in the sense that it is formed and disbanded on the same day of elections: it learns to optimize time and procedures while already in action and often shows more flexibility and discretionary power than it'd be strictly allowed by norms and legislation, in order to prevent mistakes due to fatigue or lack of attention. Its "professional culture" is easy to acquire and available to almost anyone: the practices related to casting a ballot become, in the course of election day, a well-oiled "machine". When this voting machine works, be it paper-based or electronic, it should become sort of invisible: its efficiency and its acceptance by the citizenry is signified by its *disappearance* in the sense that it becomes a *routine* taken for granted, and not an "issue".

At present, the complex and time-consuming bureaucratic procedures related to data management are described as cumbersome and old-fashioned: a simplification of the procedures related to electors identification, ballots count and register filling would definitely be welcome.

Above all, both scrutinizers and citizens explicitly and implicitly stress the need for adequate information: switching to electronic voting implies a significant change in a long established and framed routine. A new habit has to be created from scratch and it cannot be learned "by trial and error" as one might find acceptable in other technological settings. To smooth the transition to e-voting this preliminary study suggested that:

- the touchscreen should show some continuity with the paper ballot to reduce the need for cognitive re-adaptation;
- appropriate instruction should be ensured to both electors and scrutinizers: their confidence with the new system can be enhanced by open trials;
- special consideration should be granted to senior citizens: the care that institutions show towards this group will be reflected in the appraisals of many others.

3.2 Are we ready to vote electronically? Attitudes and technical skills

Alongside the "qualitative" investigation, a preliminary "quantitative" survey was carried out by means of telephone interviewing to assess the interest of the population in changing the voting procedures. The sample (2561 respondents) was representative of the adult population of Trentino, controlling for age, sex and geographical distribution. The aim of this study was to consider attitudes towards electronic voting as well as practical technological ability. The latter was measured by an index created on the basis of statements related to the use of common electronic appliances requiring skills similar to those needed for e-voting. Approximately 10% of the respondents turned out to be barely familiar with technology and a further 6% to be very unacquainted with menu-like procedures. Those who might be impaired in the use of electronic means are mostly elderly people, retired, with no or very little education. The attitudes toward electronic voting, or rather, to whatever the respondents thought electronic voting to be (as they had never experienced it in elections), are summarised in Figure 1.

How much do you agree with the following sentences?	**%**
• Voting procedures should inevitably be changed, sooner or later	70,3
• Electronic voting is a good idea, but I believe it'd be difficult to implement	58,2
• Electronic voting might eliminate contentions in interpreting voters' will	55,9
• Electronic voting might increase abstentions	54,4
• Electronic voting might lower the mistakes that today cause ballots to be invalidated	53,2
• Electronic voting is a dangerous solution as it'd be prone to vote tallying that can't be easily demonstrated	42,0
• With electronic voting there'd be no tangible proof of my vote	36,5
• Electronic voting wouldn't fully guarantee that the ballot is secret	36,1
• People are ready to switch to electronic voting	28,2
• I don't trust technology and therefore I don't trust electronic voting	27,9

Figure 1: Attitudes toward electronic voting (% of answers "agree" and "strongly agree", *n*=2561)

These attitudes confirm some of the beliefs already found via the focus groups, such as the fear that some segments of the population might not be ready to vote electronically, thus increasing abstentions; the desire that certain common mistakes and controversies will be eliminated and a feeling of the inevitability of change. However, citizens are on the whole in favour of voting electronically even in the near future, as Figure 2 shows. It's mainly professionals, students, educated people approximately below 50 years of age who are enthusiastic about e-voting (more than 65% are in favour), whereas elderly, retired citizens with no education show very little interest (less than 40% are in favour).

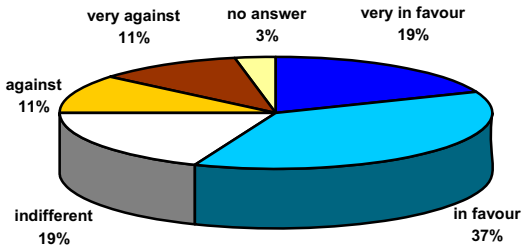

Figure 2: “Should electronic voting be adopted for the next provincial elections, would you be in favour or against this idea?” (%, *n*=2561)

The voters’ openness toward voting electronically in the next elections appears to be more related to their attitudes than to specific socio-demographic characteristics: sex, social class, education and even age have little or no impact on the will to use an electronic ballot, when technological ability and attitudes are controlled for. Young people are more inclined to technology but seem to be little interested in politics; on the other hand, senior citizens are less confident with electronic methods but are very motivated towards participating in elections, as they feel it to be a duty, not just a right. Education level has a limited direct impact on the will to vote electronically: only those who received no education, controlling for age and technological ability, are significantly less in favour. The size and the level of development of a town also have, perhaps unexpectedly, almost no influence: this indicates that smaller, rural and peripheral locations are likely to accept a switch to electronic voting at the same pace as urban areas, despite being conditioned by more “traditionalism”. What really determines the acceptance of electronic voting is the image of the strengths and pitfalls of the system: trusting or distrusting this unknown and never experienced means being the most powerful incitement or deterrent.

The quantitative preliminary study also suggested that:

- citizens are generally in favour of adopting electronic voting and their expectations are mostly positive, though some doubts remain and should be cleared before this new method is adopted;
- the fear of not being ready for the change is challenged by the widespread use of electronic appliances that require skills similar to those necessary to vote electronically;
- for a campaign to introduce e-voting to be successful, it should stress the benefits and assure electors that safety is guaranteed;
- voting machines should be adapted to the electors’ needs (rather than expecting electors to adapt to voting machines) and citizens should be aware of this effort.

Once a prototype of the voting machine was ready, trials and simulations were organized in the five towns chosen for the first large-scale field test scheduled to be performed during local elections. To try the electronic ballot with the most disadvantaged social group, a sample of 80 senior citizens was randomly chosen from the registries, ensuring that their educational level was very low or null; a reference group of further 80 young and middle-aged people was also invited to the tests, on condition that they possessed at most a high school diploma. Participants in the simulation filled in a questionnaire before and after the trials and were video-recorded during the test. As a result:

- the visual layout of the screen, i.e. the position of "buttons" and the size of characters was modified
- the choice of preferences and, generally speaking, man-machine interaction, were optimized by observing how people "naturally" tend to cast a vote by means of a touchscreen.

The flyer with instructions for the correct use of the new form of ballot were also submitted to non-experts for concept-testing via focus-groups and in-depth interviewing.

This complex but continuous exchange between the efforts of the technological team, the law standards required and guaranteed by the electoral bureau and the contribution of citizens themselves helped to develop a low-impact system which was ready to be put to trial in May 2005.

4 Trialling electronic voting: evaluation of the social impact

On May the 8th, 2005, elections took place throughout the province of Trento to choose town mayors and councillors: this turned out to be an excellent occasion to try on a large scale the electronic voting system that had been developed. Such an opportunity had no legal value, as electors were invited to test the new form of ballot after they cast the paper one, which remained the only valid one. The 7782 electors of the five towns chosen[2] for the field test received a letter of invitation and instructions: about 74% went to the polling station and cast the traditional paper-and-pencil ballot; of those, an average of 59% (with a peak of up to 80% in one of the smallest towns) tested the electronic system, too, and were asked to answer a questionnaire after completing the trial.

On the whole the participants were very satisfied with the system (Figure 3) although some problems were reported, especially in choosing councillors, in modifying a wrong choice, and in being sure that the procedure was terminated.

[2] according to a criterion based on their size and geographical location

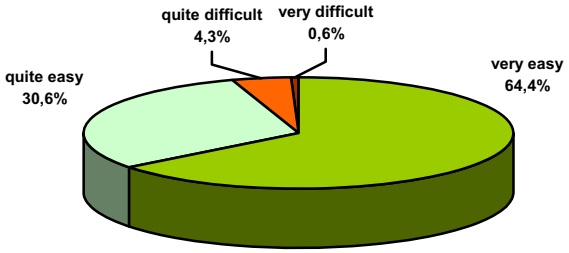

Figure 3: "How do you evaluate this new system of voting?" (%, *n*=5534)

Those who tested the electronic booth are a self-selected sample and it is reasonable to suppose that people who are very against e-voting were not among them. Nevertheless, the impression the participants got is altogether positive: 61% would be very favourable to voting only electronically already in the next provincial elections and only 10% would be very or quite against it, which is a remarkable result compared to that obtained before the field test took place (see Figure 2). The effect of exposure to different media on the perceived friendliness of the e-voting system was also considered and useful advice were taken up for the calibration of future communication campaigns. Last but not least, this field test revealed the importance of what we labelled as "scrutinizers effect", that is, the key role played by people at the polling station in reassuring and supporting electors, which leads to a higher turn-out in the electronic booth and a lower number of perceived impediments.

A second trial, on a much smaller scale, took place in November 2005 on the occasion of another round of local elections and provided a useful assessment of the modifications made to the system. Interestingly, in the town where this field test took place voter turn-out resulted in one of the highest in a ten years span, thus suggesting that electronic voting and the communication campaign that preceded it caused some kind of "Hawthorne effect" stimulating the citizens' curiosity and interest in elections. 89% of those who cast their ballot repeated their vote electronically (vs. 59% in May): though the absolute numbers of citizens involved in the two tests are very different (336 in November and 6950 in May), it is quite clear that greater attention to communication and to motivating scrutinizers significantly increases the voters' will to try electronic voting.

Voters' subjective evaluation of the system was extremely positive: none judged it to be very difficult to use and only 2% described it as "quite difficult" (compare with Figure 3). Electors who experienced some kind of trouble while testing the system relied on the assistance of scrutinizers whose support from outside the voting booth helped them overcome difficulties and resulted in a positive evaluation of the trial[3]. As with the first test, the respondents are a self-selected sample, which leads to an optimistic bias, but such a positive result indicates that the experience of using the touchscreen proved to be much easier than the image of it (as portrayed in Chart 2). The technical effort in improving the way councillors are chosen also abated the perceived hindrance in performing this operation, thus highlighting the importance of repeated tests and trials in "real world" settings to optimize the system according to actual voter-machine modes of interaction.

At present further studies are being carried out to test for the statistical significance of the trials on turn-out and on the vote cast, though from a strictly descriptive viewpoint electronic voting appears not to have impinged on attendance and the ballots electronically recorded are consistent with the paper ones, having legal standing.

5 Recalling memories: capitalising on the effects produced by the trials

A *post hoc* telephone survey on a sample of the citizens potentially involved in the first field test allowed us to further evaluate the social impact of the introduction of e-voting: recalling the memory of the elections some months after they took place helps to understand how much of this experience "remained". These follow-up interviews were aimed at monitoring the exposure to an array of media forms used during the communication campaign and to verify their effect on the decision of participating in the test. They also provided a useful assessment of the perceived trust in electronic voting: as Figure 4 shows, interviewees are altogether slightly more favourable to e-voting with respect to the first telephone interview (compare with Figure 2) and those who tried the electronic booth first hand are definitely very satisfied. Results for those who watched others e-voting are also reported, as well as the attitude of the citizens who declared not to have voted at all.

	sample	testers	watchers	non-voters
very in favour	**21%**	32%	12%	9%
in favour	**41%**	49%	39%	28%
indifferent	**17%**	8%	20%	36%
against	**14%**	9%	19%	12%
very against	**7%**	2%	10%	14%
N	***1206***	*503*	*372*	*146*

Figure 4: "Should electronic voting be adopted for the next provincial elections, would you be in favour or against this?"

[3] 61% of the interviewees answered to be *very in favour*, 26% to be *in favour*, 5% to be *against*, 2% to be *very against*, 6% to be *indifferent* to adopting electronic voting already for the next provincial elections (*n*=306).

Those who tested the touchscreen were also required to provide a subjective comparative evaluation of the traditional paper-and-pencil system and of the electronic one on a set of aspects such as user-friendliness, perceived secrecy, facility for interpretation of electors' will, proneness to vote tallying *et al.* The results show a preference for electronic voting regardless of sex, age, education and declared level of participation in elections. Consistently with the outcomes of the *pre-hoc* survey, favour towards electronic voting increases with level of education and participation and decreases with age, whereas paper-and-pencil balloting does not show any clear-cut trend related to these variables.

6 Conclusions

All through this paper we attempted to stress that studying social feasibility is a central issue in introducing such a substantial transformation as electronic voting. The impact of this innovation in a setting traditionally governed by symbolic and material customs is a very delicate matter that can be faced efficaciously only through the active involvement of all stakeholders: policy-makers, technologists, but above all citizens. We suggested a model of action research aimed at facilitating the switch from paper-and-pencil to electronic ballot, though further study is needed to provide a comprehensive assessment of the social impact. The results we presented suggest that citizens in the province of Trento are ready to accept the challenge but they need to be adequately supported by a communication campaign tailored to the needs of each social group. It is also important that more trials are conducted to help people get used to the new system before it is granted legal standing: only by "going local" and by listening to citizens it is possible to develop a voting machine truly compatible with their expectations and skills.

References

[Ed64] Edelman, M.: Symbolic Uses of Politics. University of Illinois Press, Urbana, 1964.

[Ke88] Kertzer, D.: Ritual Politics Power. Yale University Press, New Haven, 1988.

[Me02] Mercuri, R.: Explanation of voter-verified ballot systems. In ACM Software Engineering Notes (SIGSOFT) 27(5), 2002. Also at http://catless.ncl.ac.uk/Risks/22.17.html

[Se02] Servon, L.J.: Bridging the digital divide: technology, community, and public policy. Blackwell, Oxford, 2002

[SHB92] Shocket, P.A.; Heihberger, N.R.; Brown, C.: The effect of voting technology on voting behavior in a simulated multi-candidate city council election: a political experiment on ballot transparency. In Western Political Quarterly 45(2), 1992; S. 521-537

[Sl93] Slovic, P.: Perceived risk, trust and democracy. In Risk Analysis 13(6), 1993; S. 675-682

[TV03] Tomz, M.; Van Houweling, R.P.: How does voting equipment affect the race gap in voided ballots?. In American Journal of Political Science 47(1), 2003; S. 46-60

[Ve04] Venice Commission - European Commission for Democracy Through Law. Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe adopted by the Venice Commission at its 58th Plenary Session on the basis of a contribution by Mr. Cristoph Grabenwarter, 2004 http://venice.coe.int/

Session 8: Security for E-Voting

Security Requirements for Non-political Internet Voting

Grimm, Rüdiger[1]; Krimmer, Robert[2]; Meißner, Nils[3]; Reinhard, Kai[4];
Volkamer, Melanie[5]; Weinand, Marcel[6]; Helbach, Jörg[7]

[1]Universität Koblenz-Landau; [2]Wirtschaftsuniversität Wien; [3]PTB Berlin;
[4]Micromata Kassel; [5]DFKI Saarbrücken; [6]BSI Bonn; [7]GI Bonn
for further questions: grimm@uni-koblenz.de

Abstract: This paper describes the development of security requirements for non-political Internet voting. The practical background is our experience with the Internet voting within the Gesellschaft für Informatik (GI – Informatics Society) 2004 and 2005. The theoretical background is the international state-of-the-art of requirements about electronic voting, especially in Europe and in the US. A focus of this paper is on the user community driven standardization of security requirements by means of a Protection Profile of the international Common Criteria standard. An extended version of this article (20 pages) is published as technical report by the University in Koblenz (see reference list).

1 The GI and its election 2004

The Gesellschaft für Informatik (GI) is a society for computer science with presently about 24.000 members mainly from Germany. The rules for elections of the bodies of the GI are formally specified by the GI [GI03; GI04]. Since July 2003, the article 3.5.4 of the constitution of the GI allows the application of Internet voting. Here the precondition is that the Internet voting system provides the same security level as postal voting. In all cases where postal voting is admitted the election committee can decide to give members also the possibility to use an Internet voting system – as long as it is comparably secure. In summer 2004, the chairmanship (Präsidium) decided unanimously to offer both, postal voting and Internet voting for the chairmanship elections in December 2004. The election was successful. As a consequence the persons in charge decided to apply Internet voting again in 2005 for the election of the chairmanship and of the executive board of the GI. Until now the GI has voted online twice and plans to do so again in 2006.

After a market survey the GI chairpersons decided to use the POLYAS system [MM05] for Internet voting. The POLYAS system provides two authorization schemes, one based on authentication with digital signatures, the other employs PINs and user-ids instead. For better usability and simplicity, election PINs and personal user-ids were chosen for the GI election. Every GI member received a paper letter with the information material how to use the Internet voting system. In particular, the letter informed the member, that the user-id is the GI membership number. The PIN was printed on the letter and

concealed by an opaque (not transparent) sticker on the letter. The user-id and election PIN was used for registration. Finally, the letter specified the URL for the Internet voting system. Every voter who did not want to cast her vote electronically could alternatively participate by using postal voting.

The GI established a group of security experts to accompany the election and the future process of Internet voting in the GI. This group examined the specification and the documentation of the system, in particular with regard to data protection and manipulations. A main task of the expert group was to develop and enforce ad-hoc security requirements in cooperation with Micromata.

Micromata has done some minor changes on POLYAS to comply with the security requirements. Most security requirements could be met by organisational means. On a technical level, the following features were implemented

- audit proof archiving of the ballots preventing later manipulation of votes;
- separation of the electoral register from the ballot box; in particular, any shared marks were removed;
- SHA-signatures of software packages and result files.

Over 5000 members used the Internet voting system. The participation was significantly better than in several years before.

2 GI election 2005 – restructuring the security requirements

In December 2004, the Internet voting expert group of the GI decided to develop a requirements catalogue for „Internet-based elections in societies". They agreed on two preconditions. Firstly, the security requirements must ensure a security level not less than that of postal voting. Secondly, the catalogue should be short and crisp and should not exceed six printed pages. Four requirements catalogues were already available and could be used as a basis for further development: [CoE04; SCC04; PTB04]. After several iterations, a last version was published in [GI05].

The catalogue starts off with some preliminary notes and explicates assumptions under which any applied Internet voting system must ensure the security requirements. For example, it is assumed that the voter casts her ballot from an arbitrary Internet device connected to the Internet. Other assumptions are these: A non-secret name or a membership number (user-id) is applied for the voter identification. A secret alphanumeric password (one-time election PIN) is used for the voter authentication. The electronic ballot box and the electronic election register are installed on different servers. The two servers are located in different organisations. Postal voting is possible for every voter who does not want to cast an electronic ballot. The preliminary notes also define issues which are out-of-scope of the security requirements catalogue. For example, the candidate nomination and the maintenance of the list of eligible voters are not considered in the catalogue. Rules for a long-time storage of the election results are not addressed, either.

The catalogue of 2005 separates the requirements on the system development and on the election execution from those requirements on the Internet voting system itself. The requirements on the voting system itself are divided in requirements on the election servers and on the election software.

The general requirements on the system development contain requirements on the type and level of details of the system description, the security analysis and the manuals. There are especially strong requirements on the anonymity concepts. This category includes requirements on the development process, the system tests and the key management. The requirements on the election execution contain the distribution of the election PIN, the election register management and the installation as well as the de-installation of the voting system. The catalogue requires for the election servers to run a secure operating system, and to isolate the election software from all other applications. Only authorized persons may have access to the servers.

For the requirements on the election software the following categories were used.

- General requirements to an Internet voting system and its security
- Specific functional requirements to the Internet voting system
- Requirements with respect to the anonymity of votes
- Specific requirements to ensure a universal and equal election
- Ergonomic and usability requirements

The general functional requirements include the systems reliability and logging as well as the guarantee of consistent system states in case of any interruption. Specific functional requirements refer to the electronic register and to the electronic ballot box. Requirements with respect to the anonymity specify a secret, equal and universal election. The last category of requirements on the election software addresses ergonomics and usability.

3 GI election 2005 – meeting the requirements

On the basis of this agreed catalogue of requirements, Micromata was requested to explain how the POLYAS system ensures each of the requirements. Micromata has developed a new major release called POLYAS 2005 complying with the new catalogue of requirements. The main issues were:

- separation of the two servers, the ballot box and the election register;
- creation of a third server instance called the validator: the validator signs every entry of the electoral register before the elections starts; during the voting process the validator checks this signature of every voter from the register before it enables the voter to cast his ballot;
- system recovery, e. g. after system errors or client aborts during the election;
- detection of manipulations without violating the confidentiality of the ballots;
- several mechanisms to minimize possible system attacks by both, external Internet users and internal corrupted administrators: e.g. a check sum of each vote, the storage of votes as readable text and not as a database reference, splitting up the keys in a passphrase and a secret key to support the four-eyes-principle, firewalls and a „secure" operating system.
- documentation of all technical and organisational solutions to accomplish the security requirements;
- anonymous creation of the voters' PINs for the print service provider.

The technical solutions concerning error handling, recovery mechanisms, manipulation and threat scenarios were documented in detail. Organisational security solutions are based on the four-eyes–principle. At least two different persons must cooperate for administration of the systems, for starting the election application etc. The roles and responsibilities of the actors (management, administrators, voters, service providers etc.) are clearly specified in the documentation.

By applying the POLYAS system to the requirements catalogues we found out that several terms were used inconsistently. Thus, we developed a glossary including the terms election voting system, election voting software, ballot box, ballot box server, and authentication token.

Workshops in Kassel (home of Micromata) and Munich (home of one of the GI board members) revealed four new challenges:

1. Source code inspection: In order to increase trust in the decency of the software, and especially in order to identify undetected errors, Micromata and the GI expert group invited external experts to inspect the code of the POLYAS system. The inspection was not formal. Different experts of the GI community and of the Physikalisch-Technische

Bundesanstalt (PTB) inspected parts of the code on their own choice and on the background of their personal engineering experience. The code proved to be well structured. However, a set of improvements were initiated.

2. A simplified voters' guide [GIFS05]: The GI expert group specified a set of guidelines for online voters, which contains one page of general hints and thirteen easy-to-follow one-sentence rules for voters. The guidelines do not provide the illusion of a 100 percent secure client (which does not exist), but helps users to better assess their security level and to improve it on their own responsibility.

3. CC standardization of the requirements catalogue: In order to standardize the findings on security requirements the Common Criteria (CC) is the suitable framework. The GI expert group founded a sub-group to specify a CC protection profile for the security requirements of Internet voting for private societies and other non-governmental organisations. The GI would be one application field of the protection profile. This issue is discussed in chapters 5 and 6 of this paper in more detail.

4. A suitable comparison of Internet voting with postal voting: Despite the regulation of the GI elections that the security of Internet voting must be at least on the level of postal voting, these two voting methods cannot be compared in every respect. There are pros and cons with both systems, and in some respect, Internet voting is even much more secure than postal voting. For example an Internet voting system has the possibility to send an acknowledgement to the voter which informs the voter that her ballot has been stored. With postal voting the voter cannot know exactly if or if not her ballot arrives at the electoral office in time or if it arrives at all. The enforcement of anonymity is another advantage of Internet voting. Electronic ballots can be encrypted safely. Within postal voting, in contrast, it is much easier to open the well marked election letters. For a deeper discussion of this issue see [KrVo05].

4 The future of GI elections

The GI elections 2005 were a success, too. The participation was kept on the same improved level as 2004. There were no serious security attacks.

One problem was that the stickers on the paper letters were not as opaque as they should have been: very strong light was able to make the covered PINs visible. This is not a problem of the electronic system, but of the organizational implementation of the system. Another general problem is that a voting system must be able to handle differences between the number of voters that are registered as having voted and the number of votes in the ballot box. This may happen when messages between the servers get lost. The Polyas system offers protocol security mechanisms to detect such inconsistencies and fix them dynamically.

Plans for the next major release 2006 are:

- further improvement of the Internet voting protocol for a better system recovery after system failures;
- as an extension of the four-eyes-principle: implementation of an m-n threshold scheme for key distribution;
- support of EML (election markup language) for an easier configuration management;
- modified modules will help local chairs of GI subsections to administer their own elections.

Long term plans include the implementation of a rich voting client using bulletin board systems technologies. Rich voting clients allow for the implementation of security anchors in the hand of the voters.

As a consequence from this encouraging experience, the GI will continue to offer Internet voting to its members. Especially for the departments and working groups of the GI, Internet voting will be cheap, safe, and easy, and it will include much more members to execute their democratic right to elect their chairpersons.

5 International and European standards for e-voting

Discussions about the security of e-voting systems have often been led in a very emotional way. Following the falsification principle of Karl Popper the security of an e-voting system can never be proved but only perceived secure until proven otherwise. This, and the fact that anonymity in electronic processes is not an easy task, has led to numerous reports about erroneous and fraudulent e-voting systems. In order to reach confidence of the voters, developers and election operators have soon started to develop requirement documents which have often emerged to real standards. Note that electronic voting comprises the usage of voting machines and remote e-voting systems.

Germany was one of the first to have legal regulations concerning the use and testing of mechanical voting machines. The „Regulation of voting machines" [DE75; DE99] was set into place as a law on voting machines in 1975 and was changed in 1999 to allow for electronic voting machines. Currently only e-voting machines built by Nedap have passed the official tests by the German test authority PTB. These machines had been in discussion in Ireland for the national elections 2004. They are in use in several locations all over Germany. In the United States the use of voting machines is decided on a district level which makes national standards on those machines hard to push. Still the IEEE made an effort with the „Project 1583" [IEEE05] to develop such a standard in the aftermath of the 2000 Florida experiences. After a controversial debate about the draft standard, it finally was turned down and the working group is still trying to deliberate on the controversial issues.

For remote electronic voting one of the first discussions around requirements was the working group set up by US President Clinton in 2000 [IPI01]. It took place during the Arizona Primaries which was the first political election to feature e-voting for participation by the general public. The report of this working group defined a number of quality criteria for remote e-voting software to be met for a successful usage. In the succession of the Arizona experiment another project evolved: the election mark-up language standard. This has been developed by companies engaged in e-voting under the umbrella of the standardization organisation [EML05]. In Germany the national metrology institute PTB developed a criteria catalogue for networked polling stations in order to support the W.I.E.N. project. [PTB 04]. It uses a similar methodology like the one used for voting machines. This catalogue may serve as a basis for evaluation of Internet voting systems in Germany.

The largest effort to come to a common understanding by a set of criteria for both, remote electronic voting and voting machines, has been conducted by the Council of Europe [CoE04]. With the help of delegates from all 48 member states it has developed a set of legal, operational and technical standards on electronic voting. It is the most comprehensive and universal standard to date.

There are even many more collections of requirements with different foci. Nevertheless hardly any of the e-voting systems have ever been checked with reference to an international standard. The perceived security of the systems is most often based on some kind of an independent audit by experts. This lack of transparency can only be improved by proper documentation in the framework of an internationally accepted standard.

6 The CC approach of protection profiles

The Common Criteria (CC) is an international standard (ISO 15408) for computer security. The official name is „The Common Criteria for Information Technology Security Evaluation". Its purpose is to allow users to specify their security requirements, to allow developers to specify the security attributes of their products, and to allow evaluators to determine if products actually meet their claims. Thus, the CC distinguishes three groups: the customer, the developer and the evaluator. Independent of these three groups a certification authority certifies the related statements.

The Common Criteria results from a standardization of national security criteria from different sources, starting with the „Orange Book" of the US DoD 1985. The criteria are improved continually. At the moment the official Common Criteria version is the version V2.3. Today many nations (e.g. Germany, France, UK) have introduced the Common Criteria to define and certify IT security products and procedures. There is a growing list of nations which at least accept the CC-certificates (e.g. Spain, Greece, Italy).

The CC contains three parts: the Introduction and Common Model (part 1), the Security Functional Requirements (part 2), and the Security Assurance Requirements (part 3):

There is also a related document, the „Common Evaluation Methodology“ (CEM). The CEM guides an evaluator in applying the CC. They convert the assurance requirements of the CC to concret verification tasks. The CC defines two most important document types: the Protection Profile document (PP), and the Security Target document (ST).

A PP is a set of security requirements for a category of possible products, so-called Targets of Evaluation (TOE) that meet specific consumer needs. The requirements are independent of technical solutions, that is, PPs leave the technical implementation open. A PP distinguishes between security functional requirements and security assurance requirements, described in a very specific (semiformal) way defined by the CC. In addition there is a description part which describes the security concepts and the threats. In particular the description part maps requirements to the threats.

An ST document is to be created by a system developer, who identifies the security capabilities of his/her particular product. An ST may claim to implement zero or more PPs.

Both PPs and STs can go through a formal evaluation. The evaluation is done by an accredited laboratory. An evaluation of a Protection Profile is a pure document check. It simply ensures that the PP meets various syntactical and documentation rules as well as sanity checks. Therefore the evaluator has to check whether the set of requirements is exhaustive and self-contained. Successfully evaluated PPs are accredited by the German Federal Office of Information Security (BSI). Certificates for protection profiles are recognized and published internationally on the Common Criteria Portal.

A Security Target, in contrast, compares a concrete product with an ST document. The purpose of an ST evaluation is to ensure that the actual product (the TOE) meets the security functional requirements described in the Security Target. An ST can be based on one or more Protection Profiles if all included PPs are evaluated and if they have received a certificate of compliance. The evaluation insensitivity of the related TOE depends on the Evaluation Assurance Level (EAL), fixed as a minimum level in the ST or PP. The CCs predefine seven test depths (EALs) whereby Level 1 is the lowest and Level 7 the highest level. Level 4 is the highest level for typical commercial products and includes the source code evaluation. From level 5 and higher we need more and more formal specification documents.

A Protection Profile contains seven main parts: the Introduction, the TOE Description, the Security Environment, the Security Objectives, the Security Requirements, the Application Notes and the Rationales. A PP starts with the introduction part which contains document management and overview information. This part should help a potential user of the PP to determine whether the PP is of interest or not. The TOE description provides context for the evaluation to improve the understanding of the security requirements. The statement of TOE security environment shall describe the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed, i.e. assumptions about the environment, threats, and organisational security policies OSP (the OSP cover all regulations or laws which have to be supported by the TOE) . The statement of security objectives are

deduced from the security environment. The security requirements part of the PP defines the detailed IT security requirements to be satisfied by the TOE or its environment. The security requirements are the text blocks predefined in the CC-catalogue. The application notes are optional. They may contain additional supporting information about the construction, evaluation, or use of the TOE. The rationales part of the PP presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. This is a self check chapter for the PP editor.

The CC is a tool to build standard documents. The evaluated and certificated Protection Profiles are registered, available and accepted on an international level. The PP concept offers the customers the possibility to define their security requirements and standards for products. Thus, product developers are able to implement products that meet the customers' needs.

7 Summary and Conclusions

Internet voting has to guarantee the anonymity of voters and the authenticity of their votes. These two security requirements seem to be contradictory, but in fact they are not. Early solutions by homomorphic cryptographic functions or blind signatures have fascinated the academic community. However, related solutions were not accepted by a broad user community. Therefore, the German „Gesellschaft für Informatik" (GI) has decided to learn from earlier experiences and to try out a simpler version of Internet voting. In order to make this project serious, the GI – together with a professional system provider – developed an existing solution further and performed two elections electronically with the system while it was developed.

Besides other measures to improve security and transparency like source code inspection and usage guidelines, a set of security requirements was formulated and refined by public and expert discussion. Voting principles are basically the same in all democratic societies of the world. Therefore, it makes sense to formulate the security requirements in a way that the international community can share the experience and take influence. A standardized way of security requirements created by a user community is given by the instrument of a Protection Profile of the Common Criteria [ISO99].

We have initiated a working group to work on such a Protection Profile. Realistic applications are groups which have a need for decisions but do not often meet physically. Examples in the academic community are IFIP technical committees and working groups, IETF and W3C committees, and distributed project teams. In the economic life staff and workers councils and shareholder groups could profit from Internet voting. We expect a first published version of a Protection Profile for non-political Internet voting by late summer 2006.

References

[CC99] Common Criteria, Security Evaluation. Version 2.1, August 1999. ISO/IEC 15408:1999. And Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999. www.bsi.bund.de/cc/. See also www.commoncriteriaportal.org [6.4.2006]

[CoE04] Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum, Straßburg, 2004. http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf [6.4.2006]

[DE75] Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland („Regulation of voting machines for elections of the German and European parliament"), 03-09-1975

[DE99] Update 1999 of Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, Last update 20. 4.1999, http://bundesrecht.juris.de/bundesrecht/bwahlgv/ [6.4.2006]

[EML05] OASIS: Election Markup Language v.4. Last modified: January 24, 2005. http://xml.coverpages.org/eml.html [6.4.2006]

[GI03] Satzung der GI („Constitution of GI"), Bonn, 2003-07-21. http://www.gi-ev.de/wir-ueber-uns/unsere-grundsaetze/satzung/ [download 06 Jan 2006].

[GI04] Wahlordnung der GI („Regulation of Voting for GI"), 2004-09-21, Bonn, http://www.gi-ev.de/wir-ueber-uns/leitung/wahlen-und-ordnungen/ [6.4.2006].

[GI05] GI-Anforderungen an Internetbasierte Vereinswahlen („GI requirements for Internet based elections in non-governmental organisations"). 4. August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf [6.4.2006]

[GIFS05] Gesellschaft für Informatik and F-Secure Deutschland: Information für GI-Mitglieder zu möglichen Sicherheitsproblemen auf Clientseite bei Vorstands- und Präsidiumswahlen mit dem Online-Wahlverfahren. („Information about possible security problems for clients of online-voting"), 2005.

[Grim06] Grimm et al. (2006): Security Requirements for Non-political Internet Voting. An extended version (20 pages) of this article is published as technical report by the Institute for Information Systems Research of the University in Koblenz. 2006. http://www.uni-koblenz.de/FB4/Institutes/IWVI/AGGrimm/Downloads [21.4.2006]

[IPI01] Internet Policy Institute (2001): Report on the National Workshop on Internet Voting, Issues and Research Agenda. March 2001. http://news.findlaw.com/hdocs/docs/election2000/nsfe-voterprt.pdf [6.4.2006]

[KrVo05] Krimmer, R.; and Volkamer, M.: Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In EGOV (Workshops and Posters), 2005. 225-232.

[MM05] Polyas Online Voting Solutions – Online-Wahlen für Verbände und Vereine. Kassel. http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf [6.4.2006]

[PTB04] Physikalisch-Technische Bundesanstalt (PTB, 2004): Online Voting Systems for Nonparliamentary Elections – Catalogue of Requirements. Technical Paper PTB-8.5-2004-1, Berlin, April 2004. http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf [6.4.2006]

[SCC05] IEEE Standards Coordinating Committee 38 (SCC 38, 2005): Voting Standards. Project 1583 – Voting Equipment Standard; and Project 1622 – Electronic Data Interchange. http://grouper.ieee.org/groups/scc38/index.htm [6.4.2006]

Online Voting Project – New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles

Klaus Diehl, Sonja Weddeling

T-Systems Enterprise Services GmbH
Onlinevoting
Pfnorstr. 1
64293, Darmstadt, Germany
{klaus.diehl | sonja.weddeling}@t-system.com

Abstract: For several years, T-Systems Enterprise Services GmbH has been researching the creation of a highly secure voting system that meets the latest cryptological standards. With exclusive responsibility for the W.I.E.N (Wählen in elektronischen Netzwerken, Voting in electronic networks) research project supported by the government since 2005, T-Systems are studying the implementation of online voting in non-parliamentary elections. The voting system previously designed in this project was subjected to a thorough review by a renowned cryptologist from a German university in the summer of 2005. Some encryption processes were then modified, resulting in a highly secure voting protocol with the provisional working title of t-voting, which is simpler and quicker to implement. By adding important new steps within the core architecture, the strenuously disputed claims to the publicness of voting and its transparency are demonstrated. A public notice displayed on the bulletin board gives voters an overview of votes cast. Considering that online voting is seen as an alternative to postal voting, this actually increases the element of being "public". The principle of universality is augmented in online voting as the access options are simplified, which means that more voters can participate in the election.

1 Introduction

Since 2001, T-Systems has been researching the creation of a highly secure voting system that is virtually fraud- and interference-proof from cryptological perspectives with the assistance of the PTB (*Physikalisch Technische Bundesanstalt* - national metrology institute providing scientific and technical services) and other prominent institutes. T-Systems has been exclusively responsible for the W.I.E.N (*Wählen in elektronischen Netzwerken*, Voting in electronic networks) research project supported by the Federal Ministry of Economics and Labour since the start of 2005. This project involved the implementation of online voting at networked polling stations in non-parliamentary elections and its examination from a legal, technical and organizational viewpoint. During this project, past experiences in the field of electronic voting were

documented. In fall of last year, the voting system developed in the W.I.E.N. project using renowned cryptologists underwent a security review. The scientists came to the conclusion that the workflow of the core architecture was too laborious in various places and also contained security flaws. After a report was produced, the voting system was extended to include important cryptological add-on modules and the client-server architecture optimized. The result is a modified voting system core that incorporates state-of-the-art technical security and has been co-developed by the PTB. The environment of the voting system, which affects voting preparation, implementation and post-processing, has remained unchanged, as has the credo of an information-based division of powers and the use of blind signatures. The voting system being developed by W.I.E.N. was completed at the start of 2006, thereby concluding the project.

The newly developed and implemented voting system should now undergo a certification process based on the common criteria as per the ISO/IEC 15048 standard in cooperation with an accredited testing centre and the BSI (*Bundesamt für Sicherheit in der Informationstechnik,* Federal Office for Information Security). It is initially planned to create the protection profile, which is subdivided into three individual protection profiles relating to voting preparation, implementation and post-processing. The legislative instances for non-parliamentary elections in particular, e.g. work council elections, staff council elections and social security elections should be integrated early on. Once these protection profiles are created, they should be certified by the BSI to form the basis for their registration. When this process has been concluded successfully, an evaluation of the system in view of the previously established requirements is planned. Lastly, the voting system should be certified on the basis of the common criteria and also be subject to a comprehensive check by the PTB simultaneously to create a basis for legal legitimization.

In addition, the voting system developed in W.I.E.N., which is limited to the voting of networked polling stations, was and is being extended to include a remote voting system. The security requirements of such a system should first be examined and defined, and based on the results obtained software engineering should be the next step. The online voting project will perform business management studies of remote voting and the creation of its legal basis in parallel.

2 Adherence to Voting Legislation Principles

2.1 Voting legislation principles for publicly regulated elections with emphasis on the publicness of the election

For the analysis of the legal principles of elections, the voting legislation principles of Art. 38 of the Constitution of Federal Republic of Germany, federal, state and municipal voting laws and regulations for non-political elections (staff council, social security and works council elections) must be applied. The first principle is that of **universality**, in which the electronic voting must be equated to postal voting. A general election is one in which all citizens can participate regardless of their status or gender, and no voters are

excluded from voting unwarrantedly. Through improved access options such as e.g. the remote voting procedure which take account of the increased mobility and individualization of voters, the principle of universality is increased. The next principle is that of **directness**, which means that all entitled voters – without the interposition of electors - must cast their vote in the polling station themselves. There must be no further contact between voters and electoral candidates after voting. This voting principle generally poses no problems for Internet voting. Another principle is **freedom** of election, which means no pressure of any kind can be exerted on the voters, such as bans, sanctions or discrimination, to force them to participate in the election or to cast their vote for a specific party. Freedom of election is protected by the principle of confidentiality. The principle of freedom also includes permitting the possibility of casting an intentionally invalid vote. Next is the principle of **equality**, which means that all voters have the same number of votes with the same count and success value. The last principle refers to the **secrecy** of election. All voters must be able to cast their vote such that no-one can determine how they are voting or have voted. Voters must therefore be unobserved while casting their vote. In addition to the voting legislation principles expressly mentioned in Art. 38 I of the Constitution, there are unwritten constitutional voting principles, for political elections at any rate: publicness of election, simultaneity, comprehensibility and freedom of charge. The **publicness** of the voting process including the monitoring of the voting result is one of the most important tools for adhering to the principle of liberty. Publicness permits transparency and monitoring in elections and is necessary for all voting stages. This begins with voting preparations: polling dates and locations are publicized, the parties present their candidates publicly, electoral registers are displayed publicly and polling stations are made publicly accessible. Voting itself is a public act, but the casting of votes is secret. Finally, the determination of the election result and its publicization are also public. Votes are counted by the members of the electoral committee at a public meeting. The process of obtaining the voting result of both votes cast in person and the postal vote must be traceable for all citizens. Publicness must therefore also apply to the determination of the result.[1] Public monitoring is performed by the electoral committee, but also by any member of the public who attends. Remote Internet voting from a computer at home removes the location of voting from public view and should therefore primarily be used only as an addition to voting at the polling station.

The principle of **comprehensibility** of an election means that the act of voting must generally be simple and traceable for voters. If voting machines are used, the electoral committee must be provided with as much training material and technical expertise to allow it to guarantee and monitor the correctness of the voting process, which is its duty. Voters must also examine the casting of votes using voting machines.

[1] [KA04], p. 29.

Another point is the **simultaneity** of voting, which is still strenuously disputed in postal voting. There is a distinct advantage to Internet voting here, as in comparison to postal voting, which is generally a pre-vote, this permits the simultaneity of votes cast in person and remote voting.[2] Lastly, **freedom of charge** of election is an element of the democratic principle – voters must not incur a cost through exercising their democratic right to vote.

2.2 The new voting system and voting legislation principles

Public monitoring of digital voting both in person and remotely is problematic. From constitutional perspectives, the replacement of visual and comprehension monitoring by electoral boards and other members of the public (as witnesses etc.) is not possible.[3]

The voting system developed previously in the W.I.E.N. research project conformed to the principles of the Federal Electoral Law, which was implemented through the information-based division of powers and the use of reliable voter identification via a qualified digital signature.[4] By adding the bulletin board in the modified voting protocol, the strenuously disputed claims to publicness of election and its transparency can now be demonstrated. A public notice displayed using the bulletin board gives voters an overview of votes cast and can track voting live on the Internet if the electoral organizer wishes. Considering that online voting is seen as an alternative to postal voting, this actually increases the element of publicness. The principle of universality is increased in online voting as the access options are simplified, which means that more voters, including e.g. those impeded due to professional or health reasons, can participate in the election.

The public must be able to monitor the correct implementation of the election at all times. For this reason, they have read access to all content on the bulletin board. Only the voter status is not visible here if voting policy precludes this, which is to be assumed. The bulletin board is a passive data memory. This means that it cannot record or establish any proprietary communications. In this context, the bulletin board is viewed more as an instance as it does not participate in the newly introduced T-Voting voting procedure like the other roles. The role of the bulletin board is to make all necessary information available for implementing the voting process, taking this entitlement and access concept into account. As with a bulletin board, the data can be either read or written here depending on the rights of participants. Due to the restrictive nature of this concept, it is not possible to subsequently modify data that has already been written.

The role of the public refers to e.g. the following groups of people in works council elections:

- Entitled voters
- Unions represented in the company, or the relevant union representatives
- Employers

---

[2] [KA04], p. 34.
[3] [KA04], p. 30
[4] [BB00], p. 4.

During the voting preparation phase, the public has the option of contesting the electoral register. The 'notice' of the electronic electoral register and the process for contesting the register are already regulated in the applicable electoral regulations of the Works Constitution Act. During the voting stage, the public have no access to the data on the bulletin board. The participation of the public in the vote counting process, which is subdivided in turn into the mixing of votes and the subsequent counting of votes, is possible. The vote result can be published via the bulletin board for the user group of the public role after the votes have been counted.[5]

Public participation in the physical counting of votes is not possible due to restrictions of the medium as the votes are tallied by a computer program. However, to perform the entire process of electronic vote counting with the involvement of the public, once the electronic ballot box is closed vote counting is introduced with the process of vote mixing and the subsequent counting of votes by projecting attendance and determining the result at the polling station.

3 Technical Modification of the Voting System

3.1 Previous Voting Protocol

The voting protocol devised previously in W.I.E.N. was based on the voting protocol developed in 1993 by Fujioka, Okamoto and Ohta entitled "A practical secret voting scheme for large scale elections"[6]. This voting system primarily entails the physical and administrative separation of the electoral register and electronic ballot box. Specifically, the W.I.E.N. voting system consisted of four server services which are each linked with a database for storing persistent data. The relevant data memories, which are relational databases in their basic structure, were:

Distributor The distributor is used as a server service for transmitting the electronic constituency data. Using this, voters can connect to the authorized electronic electoral register (Validator) and the assigned electronic ballot box (Psephor) via the voting clients

Mandator In an election with voter ID/voter passport as a form of identification, the Mandator is responsible for outputting the keys of the voter

Validator The Validator provides the electronic electoral register for a specific election. Voters can also use the server service to log into the electronic voting system. The electoral office server releases the voting documents (ballot slips). It also confirms the blind vote.

[5] [PO06], p. 12 ff.
[6] [FU93], p. 244-251.

Psephor The data model of the Psephor contains the electronic ballot box. It manages the encrypted electronic votes and releases the ballot record in counting mode.

Voting client The voting client is used to determine the identity of voters, display the ballot slip, control communications, conceal and reveal information, and cast votes.

The voting protocol propagates the use of a blind signature procedure and other cryptographic procedures that protect cast votes from manipulation and unauthorized viewing. This voting protocol is still based on an encryption using public and private codes. Online voters are uniquely identified using a qualified digital signature.

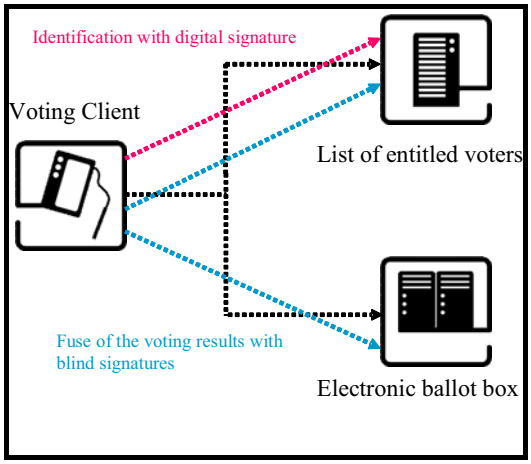

Figure 1: Principle of information-based division of powers

3.2 Newly implemented voting protocol

The voting system previously designed in this project was subjected to a thorough review by a renowned cryptologist from a German university in the summer of 2005. Some encryption processes were then modified, resulting in a highly secure voting protocol with the provisional working title of t-voting, which is simpler and easier to implement. However, the main principles of the previously developed architecture and the technologies used have remained the same.

The voter list server that issues voters with vote confirmation certificates using a blind signature[7] was also retained. Parts of the newly implemented cryptological techniques were examined back in spring 2005 using several voting tests and a legally valid test vote. In spring 2006, this voting system is also to be used for several works council elections and an Executive Staff Representation Committee election in the Deutsche Telekom group. Significant new developments include the addition of further participants. As a result, there is an interposed mix net, which separates the encrypted votes cast from the identity of the voter and stores these in random order. In addition, a bulletin board was integrated that acts as a bulletin board and shows the votes cast for everyone to see. Everyone can read messages published, but only authorized parties can store messages there. It is still not possible for anyone to delete or overwrite messages once they are written. Another element is the connection of a Tallier, which is responsible for counting the encrypted votes as a separate instance. All new developments were connected to the existing voting environment, including the administration modes.

[7] cf. [CH84]

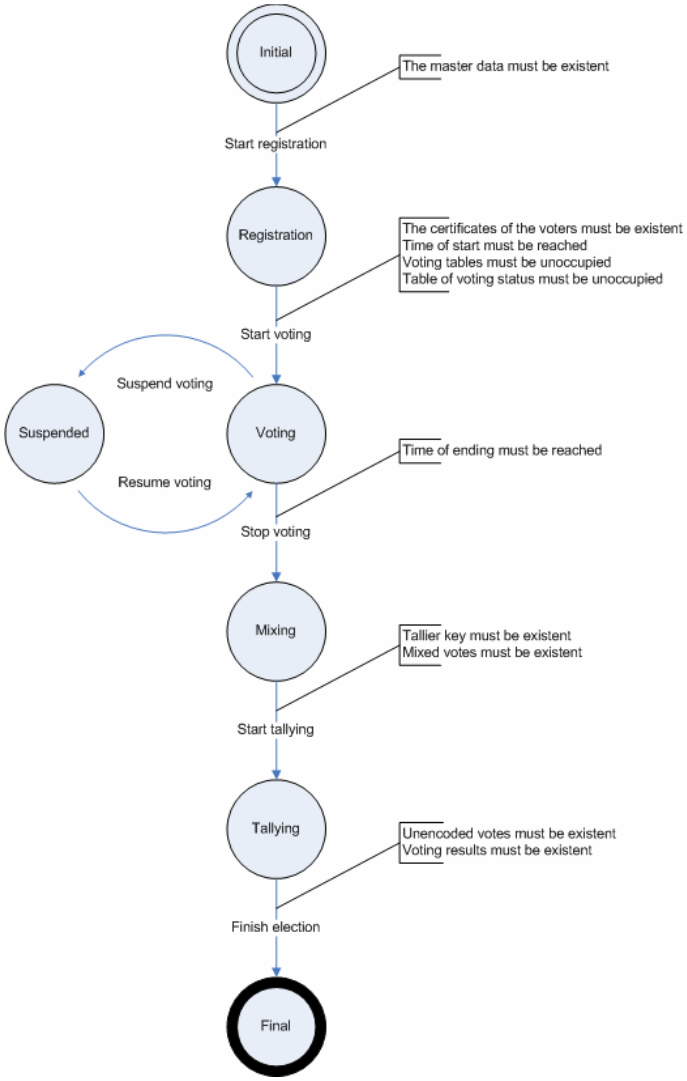

Figure 2: T-Voting phase model

The security requirements for electronic voting systems are not standardized, but science is agreed on a certain number of requirements:

Accuracy:

- A valid vote cannot be changed
- All valid votes are counted
- Invalid votes are not counted

Democracy:

- Only entitled voters can vote
- Each voter casts only one vote

Confidentiality:

- Anonymity: It is not possible to link a vote to a voter
- Untraceability: No voter can prove that he/she cast a specific vote
- A voter cannot be forced to cast a specific vote
- All votes remain secret up to the end of the election

Verifiability:

- Universal: Everyone can verify that all valid votes were counted
- Individual: All voters can verify that their valid vote was counted

The protocol uses blind signatures as per David Chaum. This mechanism prevents the signatory from being able to read the message to be signed. Another anonymization technique is the mix net as per David Chaum. Essentially, a mix net receives a number of messages, encrypts them and forwards the new messages in random order. The network thereby breaks the link between the incoming and outgoing messages. To ensure confidentiality and authentication, public key systems are used, e.g. RSA from Ron Rivest et al.

The system requires the following assumptions:

A trustworthy Public Key Infrastructure (PKI) is available and is used. All public keys are validated. A certification office issues relevant PKI certificates. This implies that all encryptions are performed using the correct public keys. All parties participate in the PKI. The cryptography used is strong and virtually unbreakable.

For communication, a protocol such as e.g. TCP/IP is used that secures the arrival of messages. We also assume that communication is protected by a protocol such as e.g. PKI-based TLS, which guarantees the reciprocal authentication of parties and the confidentiality of communications.

The registration stage is completed correctly.

There is trustworthy access control of the voting booth. This ensures that only entitled voters enter the booth, and that there is only one person in the booth at a time. The booth is constructed so that it is impossible to observe the voting process. This includes side-channel attacks (e.g. via power usage analysis).

The voting booth, mix net and bulletin board are considered trustworthy.

The voter, Validator and Tallier are not trustworthy. A valid vote is one that is in the correct form, is signed by the Validator, is encrypted in the correct order using the public key of the counter and the mix net, and is published on the bulletin board.

4 Conclusions

Through changes to the voting system developed previously in the Online Voting Project, most legal reservations against electronic voting were rebutted. The voting protocol became simpler and faster to implement, but most significantly now offers better integration of the general public through the use of a bulletin board. Previously existing technical security flaws were also eliminated. This brings us one step closer to our objective of making electronic voting feasible at networked polling stations in the short term and using any terminals without any technical, legal or organization problems in the medium to long term. We are assuming that online elections in non-parliamentary elections in Germany are now within the realms of possibility.

References

[BB00] Stephan Breidenbach and Alexander Blankenagel. Rechtliche Probleme von Internetwahlen. Berlin 2000.

[BU05] R. Araujo, A. Wiesmaier and Johannes Buchmann. The T-Vote Protocol. Darmstadt 2005.

[CH84] David Chaum. Blind signature system. In David Chaum, editor, Advances in cryptology: Proceedings of Crypto ’83, pages 153–156, New York, USA, 1984.

[FU93] Atsushi Fujioka, Tatsuaki Okamoto and Kazui Ohta. A practical secret voting scheme for large scale elections. In: Jennifer Seberry and Yuliang Zheng (Publisher) Advances in Cryptology - AUSCRYPT '92, Edition 718 der Lecture Notes in Computer Science, Page 244—251. Springer Verlag. Berlin 1993.

[KA04] Ulrich Karpen. Gutachtliche Stellungnahme zu elektronischen Wahlen. Hamburg 2004.

[PO06] Projekt Onlinewahlen, T-Systems Enterprise Services. Berechtigungs- and Zugriffskonzept Bulletin Board - Szenario: Betriebsratswahl. Darmstadt 2006.

[RI04] Volker Hartmann, Nils Meißner and Dieter Richter. Online-Wahlsysteme für nicht-parlamentarische Wahlen: Anforderungskatalog. Physikalisch Technische Bundesanstalt. Berlin 2004.

Session 9: Political Views and Democratic Challenges

The Voting Challenges in e-Cognocracy

Joan Josep Piles[1], José Luis Salazar[1], José Ruíz[1], José María Moreno-Jiménez[2]

[1]Grupo de Tecnología de las Comunicaciones
Universidad de Zaragoza
María de Luna, 1
50018, Zaragoza, España
{jpiles | jsalazar | jruiz}@unizar.es

[2]Grupo Decisión Multicriterio Zaragoza
Universidad de Zaragoza
Doctor Cerrada, 1-3
50005, Zaragoza, España
moreno@unizar.es

Abstract: e-Cognocracy[MP03, MP05, Ker03] is a new democratic system that focuses on the creation and social diffusion of the knowledge related with the scientific resolution of high complexity problems associated with public decision making. Using multicriteria decision making techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings, and the Internet as a communication support, e-cognocracy resolves some of the limitations of traditional democracy and provides room for greater involvement of the citizenry in their own government. In this sense, e-voting is not limited to the choice of a given political party, but to the extraction of the relevant knowledge.

Even though e-voting systems have already been widely studied, there are still some situations not covered yet by classical bibliography, and then it becomes necessary to introduce interesting variations to the main schema. In this paper, we will present one of such occurrences (that associated with e-cognocracy), and will study the modifications needed in the traditional e-voting processes as well as the implications they have.

1 Introduction

The degree of implication of citizens in their own government has traditionally been the issue which has led to most political changes throughout history. It has been traditionally agreed that it is desirable to achieve as much involvement as possible. This involvement should be only limited by what is practical for the smooth operation of the institutions.

This has been usually limited by the access of the citizenry to the relevant information, due to the lack of both education and readily access to the critical information. However, in the last years, with the advent of computers, the information flow between people has been steadily increasing. Internet is responsible for a great deal of this new communication, and it is being widely used by the very same citizens who will elect their leaders.

It is only natural, then, that technology has evolved to assimilate this new method of exchanging information into the classical structure. Thus, electronic voting, or e-voting, was born. However, there have been no shifts in the paradigm of the decission making process, although various different proposals have been made.

One of the obstacles these methods have is the lack of technologic means to allow their implementation. We introduce here one tool to allow one of these novel ideas, e-cognocracy, to be taken to reality.

In section 2 we will introduce e-cognocracy and its main differences with other e-voting schemes. Section 3 provides a description of our proposed voting system, as well as a proof that it satisfies the requeriments for its use in e-cognocracy. We offer in section 4 the details of our implementation and actual deployment of the system. Finally, in section 5 we provide the final considerations and future job within this project.

2 From e-democracy to e-cognocracy

Although Western societies have mainly opted for the "democracy" in their governance systems, in recent years there has been increasing discussion of a certain democratic fallacy, because this form of representation no longer meets its initial end, which is of course the participation of the citizens in their own government. Thus, many voices have been raised demanding greater involvement of the citizenry in the governance of society[Rob04]. One of the proposals suggested to improve this participation of citizens is e-cognocracy[MP03, MP05, Mor06]. It is a new democratic system employed to create a new, more open, transparent, civilized and free society that is at the same time more cohesive and connected, and more participative, equal and caring.

e-Cognocracy not only provides room for greater involvement of the citizenry in their own government and resolves some of the limitations of traditional democracy, but it also focuses on the process by which knowledge related with the scientific solution of problems is created and socialised. To this end, it uses multicriteria decision making techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings, and the Internet as a communication support.

Among the many tools needed to fully develop e-cognocracy, we will focus in e-voting, as it is the first needed to gather the information supplied by the citizens. Most known e-voting processes are limited to the technological aspects associated with the choice of a given party. However, e-cognocracy is focused on the extraction of the relevant knowledge, including the analysis of the individual and social learning derived from the scientific resolution of the problem, and this new orientation requires new technological features[Lot03, RH03].

From the point of view of the voting process, the key element introduced by e-cognocracy is the linkability of votes. In a traditional voting system, whenever the citizenry is asked to be part of a decision making process, a voting process begins.

This process starts with an information gathering phase. In it, each citizen is given the maximum amount possible of information from each of the interested parties (typically, political parties). This usually lasts for several weeks, in order to let every citizen get as much information as possible.

During that period there is very little feedback (if any) from the citizens who will partake in the votation. There are polls designed to get an idea of the actual tendencies, but they affects a very small percentage of the electorate. This, in turn, leads to a lost of interest, as the only really important moment is the voting itself.

In order to get the knowledge seeking process, we divide each votation in several rounds. Each voter can cast his vote in as many rounds as the voting process determines (but only once each round). After each round partial results are published, and more information is provided to the citizens.

For the actual results of the votation, only the last vote cast by a citizen is taken into account. However, all the history of different votations is preserved associated to the vote but not to the voter. This way, there is some information available about the trail each person followed until he arrived to his final decision.

Individual trails are never published, as they could compromise the secrecy of the voter. For instance one could be paid to vote first A, then B, then C and finally D. As the amount of rounds increases, the number of possible combinations becomes big enough to be relatively sure that only one person followed one given track. However, those trails give very valuable information which can help to detect the causes of the changes in opinion (e.g. not only that people switched from A to B, but also that most people switched after a certain event).

Also, people are encouraged to discuss their views in open forums, either anonymously or with an identity, and the effect of those discussions can be linked to the swings in the opinion of the voters.

2.1 Characteristics of our e-voting system

Our e-voting system is born as a tool for e-cognocracy and it has the following properties, sharing some of them with classic e-voting systems[BT94, CC96]:

Precision

- It shall not be able for a non authorized person to modify any votes (that is, only each voter can cast its vote).
- It shall not be possible to remove a valid vote from the final counting.
- It shall not be possible to include a non-valid vote in the final counting.

Democracy

- Only voters in the census shall be able to vote.
- Each voter shall be able to vote only once in each round.

Privacy

- A voter shall not be linked to its vote.
- A voter shall not be able to prove its vote.
- Verifiability
- Voters shall be able to verify that their vote has been correctly accounted.

Linkability

- Two votes from the same voter in different rounds of the voting shall be linked together, but not to the voter who cast them.

3 Our e-voting system

3.1 Actors in the voting process

Voter (V): Each voter must show its preferences in a multi-choice question, and rank them numerically. For each round of the voting the census shall be constant.

Certification Authority (CA): The Certification Authority shall issue the public/private keys and certificates for each actor involved in the process, and will serve as Trusted Third Party with regard to the validation of certificates.

Database server for the Electoral Authority (DBEA): The data shall be kept in a database in a secured location, without public access.

Recount server (R): The Recount server is the only entity allowed to decrypt the votes. The Electoral Authority shall provide information enough to link the votes from the same voter, but not to track them to the actual person who casted them.

Electoral Authority server (EA): The Electoral Authority shall keep track of the census, validate the users in the voting process, and sign their votes as a proof of voting. It shall also keep enough data about the votes to know the hash of the last vote from a voter (in order to link them for the Recount server) but without actually being able to decrypt them.

In this schema it is assumed that both the Electoral Authority and the Recount server do not work together to break the system and are trusted by each other and by the users. However, this is a reasonable assumption for most cases.

3.2 Initialization

The first part of the voting process is the initialization of the actors involved. In order to keep security, both the recount server and the electoral authority shall get a new key pair and certificate each voting. If desired, the keys for the voters can also be reset, though that's not necessary.

CA Initialization. The CA shall initialize only once before the start of any voting process. It shall do so by self-signing a certificate for itself and distributing it to the involved parties so that successive certificates may be trusted referring them to it.

R's private key initialization. The Recount server must decrypt all the casted votes with its private key. To avoid possible power abuses from a single owner of this key, it is possible to split it in different shares, so that a single person has not access to the voting data without coordination and acceptance.

EA's private key initialization. The Electoral Authority shall get a certificate and a key pair in order to do the blind signatures of each vote, which shall be kept by each voter as a proof of voting. It shall generate a census with the public keys of the persons allowed to vote.

Voters' registry. The Certificate Authority shall issue a new certificate and key pair to each voter who didn't have one yet, in order to be included in the census.

3.3 Voting

1. Voter makes his choices and saves the possible vote as a "voting intention" (this intention has no value as witness at all, as one could save as many of these "intentions" as desired without actually voting).

2. Voter encrypts the vote with R's public key.

3. Voter identifies himself to EA and sends it a hash of his vote for EA to issue a blind signature of it, and a ticket made from a mix of his identity and a random value that will be signed by EA as well.

4. EA verifies the voter's identity, checking it against the census and validating the client's certificate, and checks that the voter has not already cast its vote in this round.

5. EA issues a blind signature of the vote, and a signature of the ticket, and stores them linked to the voter for future rounds.

6. Voter sends to EA the vote and the blinding factor for the blind signature ciphered for R.

7. EA sends to R the ciphered vote and secret with the blind signature of it and the signature of the ticket via a secure channel.

8. If the voter had previously voted (in other rounds), EA sends to R a copy of the blind signature of the latest vote, which will be then used by R to link them.

9. EA sends to V the signature of the ticket to prove that his vote has been stored.

3.4 Recount

1. R makes public the signatures of the tickets, and starts a claims period before the publication of the results.

2. R decrypts the original votes, and uses the secret included with it to get a valid signature from the blind signature.

3. R checks the vote with the signature obtained and verifies that it is correct.

4. R links all the votes from the same voter.

5. R publishes the results of the round/voting.

3.5 Proof of fitness for e-cognocracy

In order to be used within the frame of e-cognocracy, our voting system must satisfy all the conditions previously imposed.

Precision

- As each voter authenticates himself to EA, this implies he must have a knowledge of the private key that is impossible to fake provided we use an adecuate key length.
- As each voter gets a signature of the ticket he sent to EA, and a list of those tickets is published prior to the recount, even if R is compromised, the votes cannot be erased from the ballot, as such an action would be challenged by the voters with their tickets, which would be shown to exist in EA.

- Each vote is stored with a signature from EA. A vote cannot be inserted even if R is compromised because it would be necessary to get a valid signature, and that is not possible without the private key of EA.

Democracy

- As the votes are not sent directly to R by the users, it is EA's job to get sure that the voter is properly included in the census.
- Analogously, EA will store which voters have already voted en each round, to avoid duplicates.

Privacy

- All the information provided to R is a ciphered vote, its blind signature, and a signed ticket. None of these includes anything that could lead to track the individual who casted the vote.
- The only item a voter receives is its signed ticket. That ticket is generated randomly, and has no relation whatsoever with the actual content of the vote.

Verifiability

- Each time a vote is received, EA sends back to the voter a signed ticket. Later, when the recount starts, the list of the tickets from the votes casted is published. If a voter had a ticket not included in the list, he could use it to challenge EA and see whether it has a copy of it. It EA has a copy, then the vote should be cast again.

Linkability

- Together with each vote, EA sends to R the blinded signature of the last vote casted by the same person. At the time of the recount, R looks for each vote the one which blind signature matches the included with the vote, and it reconstructs this way all the links which allow to trace the voting history of a voter, without actually revealing his identity.

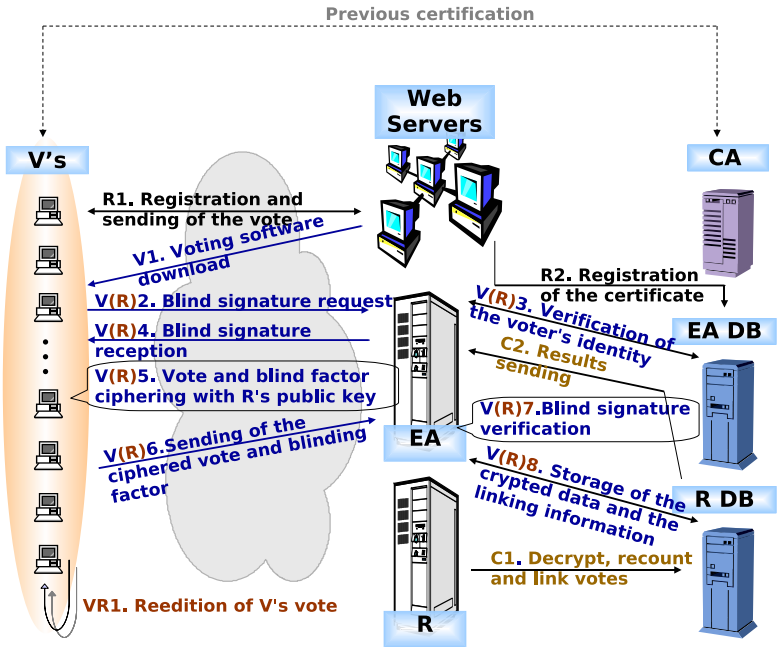

Figure 1: Overview

4 Implementation details

In order to implement the e-voting protocol, it has been chosen to use JAVA technologies, both in the client side and in the server side. This has several advantages:

- Better communication between the different components.
- More code reusability, as we can develop a series of cryptographic libraries which will be used both by the client and by the server software.
- Easy integration with the browsers.

In order to minimize the number of configurations in which the client side had to run, we decided to choose a standard web browser. In this case, it was selected Mozilla Firefox as the reference browser. It has the advantage of being open source, so its source code is readily available, contributing to increase the feeling of transparency in the process.

The browser has been completed with some libraries (JSS), needed to be able to access the client certificates which are stored in it from within the JAVA applet that will be the client software. If those libraries were not available, the user should manually add the client certificate and the CA to the JAVA application.

The application server to use will depend on the available infrastructure at the moment of the deployment. In our tests, we used Tomcat as application server. It is open source as well, and its capacity for this kind of systems is well proven.

It was chosen to use MySQL as a backend to store the data related to the votings (both the actual votes -ciphered and clear-text after the recount- and the information about the votings -question of the voting, number of rounds, period of time for each round...).

As there are two different servers (Electoral Authority server and Recount server), there could be two web and application servers, working with two different database servers. None the less, when doing the actual deployment it might happen that it is advisable to put both applications in the same application and/or web server. Likewise, it could be desirable to use two databases in a single database server. This would not be a problem, but it should be taken into account that should the server machine be compromised, the whole voting and recounting system would be broken.

All the communications between the client and the server will be both authenticated and encrypted. To achieve these goals, it will be necessary to set up an infrastructure allowing SSL and client side certificates.

4.1 Deployment details

Our group carried out a deployment of a test voting system. None the less, any future deployments should take into account that the specific details will depend on the available resources. This will be much more important if, as it usually happens, the servers are shared with other applications. The implications for the security of the system must be studied on a case by case basis.

Regarding the choice of software, we used Apache as the webserver and Tomcat 5 as application server, both of them running in LINUX i386 machines. As this was a proof of concept, the system load was expected to be very low. This allowed us to consolidate both services (the Certificate Authority server and the Recount server) within the same Tomcat instance. Likewise, both databases were stored in a single MYSQL server which was executing in the same machine with Apache and Tomcat.

There are several options available to link Apache and Tomcat. The simplest way is running two independent servers listening in different ports (in fact, it would even be possible to have them running in different machines, should the need arise). Notwithstanding this, we chose to use a tighter integration between them using the JK Connector. This technology allows to redirect queries that would normally be answered by the Apache server towards the Tomcat application server, in a way that is transparent for the user.

However, this choice makes the Tomcat application server unaware of the underlying SSL layer, because the web server forwards the request to the application server, but not the environment and security layer data. Even though the voting system cannot obtain the client certificate from the SSL layer, our protocol allows for the certificate to be sent by the client in case the server is not able to directly retrieve it.

In order to generate the certificates needed, we also set up a Certificate Authority using OpenSSL.

5 Conclusions

We have studied the novel challenges that e-cognocracy imposes upon traditional voting. We have built an e-voting system which provides the means to gather the information needed towards a more participative democracy.

As we have seen, the key to get the linkability of the votes is the separation between the Electoral Authority, who can link the chain of votes to the user but can't know the contents of each vote, and the Recount server, who can link the votes between themselves and decrypt them, but is isolated from the information about each voter.

This isn't a concern as long as both of them are trusted entities who will not work together to cheat the system.

We have also built and tested such a voting system, showing that it is feasible and that its ease of use allows for it to be widely used without any special kind of technical background.

Our future work includes developing other technological tools needed by e-cognocracy. As e-voting provides the raw data, there is still the need for a set of tools which can link the information obtained to the actual social phenomena that helps to form the results obtained in the votation. These tools includes online forum where people can exchange ideas in a controlled way, and the tools needed to extract the relevant or prevalent opinions and match them against the shifts in the voters' opinion.

6 Acknowledgements

This work has been partially funded under the research projects "Electronic Government. Internet-based Complex Decision Making: e-democracy and e-cognocracy" (Ref. PM2004-052) and "Internet-based Complex Decision Making. Decisional Tools for e-cognocracy" (Ref. TSI2005-02511).

References

[BT94] Benaloh, J. and Tuinstra, D. Receipt-free secret-ballot elections (extended abstract). In STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing, pp. 544–553. ACM Press, 1994.

[CC96] Cranor, L. F. and Cytron, R. K. Design and implementation of a practical security-conscious electronic polling system. Technical Report WUCS-96-02, Washington University, 1996.

[Ker03] Gregory E. Kersten, G.E. e-Democracy and participatory decision processes: lessons from e-negotiation experiments. Journal Multi-criteria Decision Analysis 12(2-3), 127-143, 2003.

[Lot03] Lotov, A. Internet tools for supporting of lay stakeholders in the framework of the democratic paradigm of environmental decision making. Journal Multi-criteria Decision Analysis 12(2-3), 145-162, 2003.

[MP03] Moreno-Jiménez, J. M. and Polasek, J. M. e-Democracy and knowledge. a multicriteria framework for the new democratic era. Journal of Multicriteria Decision Analysis, 12:pp. 163–176, 2003.

[MP05] Moreno-Jiménez, J. M. and Polasek, J. M. e-Cognocracy and the participation of immigrants in e-governance. In TED Conference on e-government 2005. Electronic democracy: The challenge ahead, volume 13 of Schriftenreihe Informatik, pp. 18–26. University Rudolf Trauner-Verlag, 2005.

[Mor06] Moreno-Jiménez, J.M. E-cognocracia: Nueva Sociedad, Nueva Democracia. Estudios de Economía Aplicada 24(1), 559-581, 2006

[RH03] Ríos Insúa, D., Holgado, J. and Moreno, R. Multicriteria e-Negotiation Systems for e-Democracy. Journal Multi-criteria Decision Analysis 12(2-3), 213-218, 2003.

[Rob04] Roberts, N. Public Deliberation in an Age of Direct Citizen Participation. The American Review of Public Administration, 34(4):pp. 315–353, 2004.

E-Voting in Slovenia: The view of parliamentary deputies

Tina Jukić, Mirko Vintar

Faculty of Administration
University of Ljubljana
Gosarjeva 5
1000, Ljubljana, Slovenia
tina.jukic@gmail.com, mirko.vintar@fu.uni-lj.si

Abstract: The paper presents the results of the research, focused on Slovenian parliamentary deputies' position on e-democracy with the stress on remote e-voting. It examines the difference in the position on e-democracy and e-voting of deputies aligned with the political right and left respectively. Furthermore, it considers deputies' attitude to the initiatives mediated via e-mail and assesses the risks and impact that the deputies see in e-voting. They were asked to what level they supported the implementation of e-voting and when, in their opinion, Slovenia would start e-voting tests. Finally the authors indicate the most interesting findings of the survey.

1 Introduction

There has been a great deal of discussion on e-voting over the last few years, especially within projects in Estonia, the United States, Canada, Spain, France, Switzerland, and the UK, among others. Optimists forecast greater elections turnout, pessimists warn about underdeveloped technology. The experience of other countries, which all the e-voting pioneers should take into account, is that a 'step-by-step' approach is best, which means that we should start by implementing e-voting in municipal elections, and perhaps not even in all of them.

Slovenia has not yet started any e-voting projects. An e-voting feasibility study was made in 2003, and e-voting amendments were proposed to the National Assembly Elections Act. But these amendments were not carried, which is the reason there is not yet a legislative basis that would enable this kind of voting.

Not knowing what the plans about future e-voting efforts are stimulated us to conduct a survey to find out the position of Slovenian parliamentary deputies on e-democracy with an emphasis on remote e-voting. Since the current ruling coalition consists mostly of right-aligned[1] deputies, and since, traditionally, the Right is more conservative we wanted to see, if we can expect further delays in e-voting progress. We carried out an e-mail survey, sent to all (90) deputies.

Most of regular internet users in Slovenia are among highly educated population (90%) [SO06], while, on the other side, the largest left-aligned party (Liberal Democracy of Slovenia) has more voters with higher education than the largest right-aligned party (Slovenian Democratic Party) [AP04]. This is the reason we started our survey with the hypothesis that the current ruling coalition is not in favour of e-voting, which could cause further postponement of e-voting.

The purpose of the paper is therefore to present the most interesting results, on the basis of which assumptions can be made about the further evolution of e-voting in Slovenia. First, the paper presents the current state of e-voting efforts and the research scheme. The next section presents the results of the survey and finally conclusions are drawn.

2 Presentation of the state

There is no legislative foundation to enable e-voting in Slovenia. The most important source of electoral law in Slovenia is the National Assembly Elections Act, with other electoral legislation based upon this Act. In 2003 some amendments to this Act were proposed, including e-voting, but this proposal was not supported by the Right in parliament, so the amended Act did not become law. Most of the arguments related to 'underdeveloped' technology [Ko04].

In July 2003 Government adopted a decree establishing a project council that was chaired by the Minister of the Information Society. The project group, established in December 2003, formed its first concrete guidelines for e-voting implementation in the first quarter of 2004. Three documents were prepared: (1) A scheme for a study on e-voting with a review of electoral procedures [MIS03], (2) The feasibility study: constitutional and political views on introducing of e-voting in the Republic of Slovenia [GLZ04], the Ministry of Information Society also produced a (3) Feasibility study of e-voting with the implementation proposals [Tu04]. One of the main finding of the second document was that "the use of ICT in electoral procedures is a welcome contribution to the democratization of the society." At the same time the study warned of negative effects caused by faults (e.g. technical, procedural, system) (ibidem). The review of electoral procedures for the execution of e-voting indicates that only three procedures (out of 33) exist in electronic form: (1) insight into data on right to vote, (2) electronic announcement of unofficial data and (3) electronic announcement of official data.

[1] Not all of political parties are extreme left/right-wing; we use the term left/right-aligned or simply Right/Left.

At the end of 2004 a new government took office. Its prime minister is also the president of the largest right-aligned political party. The new government abolished the Ministry of Information Society and the Government Centre for Informatics, with most of their tasks falling within the Directorate for E-Government and Administrative Processes. The current situation indicates that the e-voting project has stalled. Local elections in the present year could be a great opportunity for the e-voting pilot project, but it seems likely this will not occur. There are grounds to be anxious about e-voting projects and some other e-government projects.

It is worth mentioning that less than 10% of the Slovenian population has a digital certificate [Ce05] and the promotion of e-government services is at a low level. On the other hand, survey results [IT04] showed that 54% of respondents would participate in internet voting; it is interesting that there 58% of potential e-voters are internet users, while among non-users there are 36% of potential e-voters (ibidem).

The Strategy of E-Commerce in Public Administration of the Republic of Slovenia for 2001 to 2004 is out-of-date, so there is a vacuum[2] in the field of strategic planning of e-government, and we can only hope that the next Strategy will also include efforts to implement e-voting.

2.1 Other authors' findings

This section sets out some e-voting findings by other authors and other countries' experiences, on which our conclusions will be based.

Local e-voting. As Rivest [html1] assesses, local (county) level e-voting projects are better than national e-voting. This assessment has two arguments (ibidem): (1) there is no common point of vulnerability, which could be the target of attackers, (2) letting individual local levels of government experiment with different techniques is a good way to acquire experience.

Multiple voting. We think, that even though one of the fundamental principals of (e)-voting is 'one voter – one vote', Estonia [NEC04] makes good use of multiple voting – in the field of e-voting they consider multiple voting can prevent from vote-buying. The system only takes the last vote into consideration.

Turnout. Switzerland [So05] ascertained that internet has an impact on the group of voters aged 18 – 29 years; voters in this age group cast only 7% - 8% of all ballots, but when they had the possibility of e-voting, they cast 10% of all ballots. On the other hand, several authors think that e-voting should not be correlated to an increase of the turnout. The UK's Electoral Reform Society, for example, found that alternative voting methods (postal, SMS, internet, and digital TV) tested in local elections have not led to an increased voter turnout [ID03]. Furthermore, Norris [No02] drew a conclusion that 'e-voting would only have little or no effect on turnout'.

[2] The new strategy is in preparation.

Costs. Remmert [Re04] also sees one of the reasons for e-voting implementation in a gradual reduction of the cost. Furthermore, Van Den Besselaar et al. [VODF03] also sees a good argument for e-voting in lower costs – he finds that, in contrast to traditional voting, there are no additional costs if the e-ballots continue over more days.

3 Research methodology

The main goal of the research was to find out the deputies' position on e-democracy with an emphasis on the remote e-voting. The research was particularly focused on:

- deputies' familiarity with e-voting projects in other countries,
- their attitude to the initiatives, proposals and questions sent by e-mail,
- their opinion on e-voting effects,
- the risks they see in e-voting,
- levels at which they support e-voting implementation, and
- their assumptions on when Slovenia will start e-voting projects.

For this purpose we conducted a survey, sent by e-mail to all (90) deputies. The survey was sent on 16 January and we received 29 replies by 6 March, 16 of which came from the members of the Right[3] and 13 from the Left. Fifty-seven per cent of parliamentary deputies are aligned with the Right and 41% with the Left[4]. Figure 1 shows the percentage of members on the Right and Left and the percentage of replies:

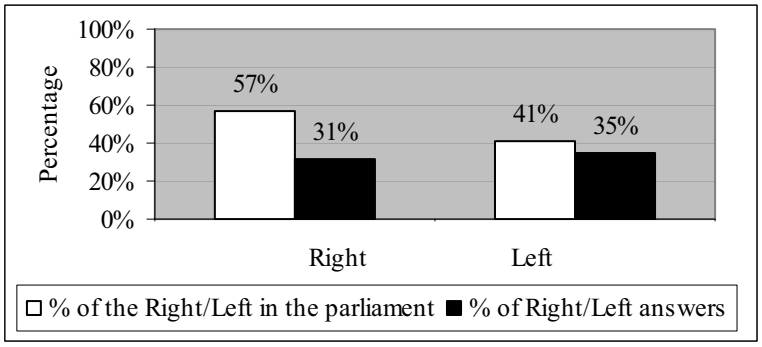

Figure 1: The percentage of the members of the Right and Left and the percentage of their answers
The percentage of returned polls is to low to generalize overall results, so there must be some reservation regarding the results.

[3] We consider that right-aligned parties to be the Slovenian Democratic Party, Slovenian National Party, Slovenian People's Party and New Slovenia, and that the left-aligned parties to be Liberal Democracy of Slovenia, Social Democrats and Democratic Party of Pensioners of Slovenia.
[4] Two representatives represent two minorities: Hungarian and Italian.

4 Presentation of the results

4.1 Familiarity with e-voting projects in other countries

As is known, some countries have already implemented e-voting in their electoral systems, while some have been implementing pilot projects for some time. We wanted to find out if Slovenian deputies were familiar with these projects.

The survey revealed that most of them (66%) had already heard something about these projects, but they were not familiar with all the details, while 14% of deputies receive information on other countries' e-voting projects on a regular basis, and 10% were not acquainted with these projects. A further 10% of them were acquainted only with the US and Estonian e-voting projects.

4.2 Attitude to the initiatives, proposals and questions mediated via e- mail

At this point we wanted to find out:

- if the deputies consider e-communication equivalent to traditional communication of proposals, initiatives and answers,
- how often they receive proposals, initiatives and questions via e-mail and
- how they treat proposals, initiatives and questions via e-mail.

The results are surprising – 48% of deputies consider e-communication equivalent to the traditional communication of proposals, initiatives and answers, while 48% of them thought that e-communication is only partly equivalent to traditional communication, and 3% thought that e-communication is not equal to traditional communication.

Most (66%) of deputies receive proposals, initiatives etc. via e-mail at least once a week, 21% of deputies receive them at least once a month, 10% receive them at least once every six months, while proposals etc. are never mediated via e-mail to 3% of deputies.

Interesting, almost half (48%) of deputies considered e-communication only partly equivalent to traditional communication, but when it comes to treatment of initiatives etc. sent via e-mail, 85%[5] of deputies say that they thoroughly studied the material and take it into consideration as much as possible. The results of the survey [De05] make our results even more interesting – in 2004 the deputies' response wasn't that high, 40% of them responded to the e-mail with a real case question from an imaginary citizen[6]. The question is, do 85% of deputies from our survey really study the initiatives, proposals etc. thoroughly? We think that this data should be taken into account with some reservations.

[5] n = 27
[6] In 14 days.

4.3 E-democracy and e-voting effects

The effects of e-voting were estimated on a scale of 1 to 5. The deputies assessed five parameters:

- citizens' e-participation influence on the quality of legislation and other decisions,
- e-voting effects on authority's legitimacy,
- e-voting effects on the turnout,
- e-voting effects on the movement in electoral body and
- the security of e-voting.

The survey revealed (Figure 2) that 66% of deputies thought that e-participation would influence the quality of legislation and other decisions – that was the opinion of 77% of the Left and 56% of the right-aligned deputies. Moreover, 28% of deputies thought that e-participation may or may not influence the quality of legislation – this is the opinion of 38% of the Right and only 15% of the left-aligned deputies. Interesting, most of the left-aligned deputies thought that e-participation would have influence, while this is the opinion of far fewer (56%) members of the Right:

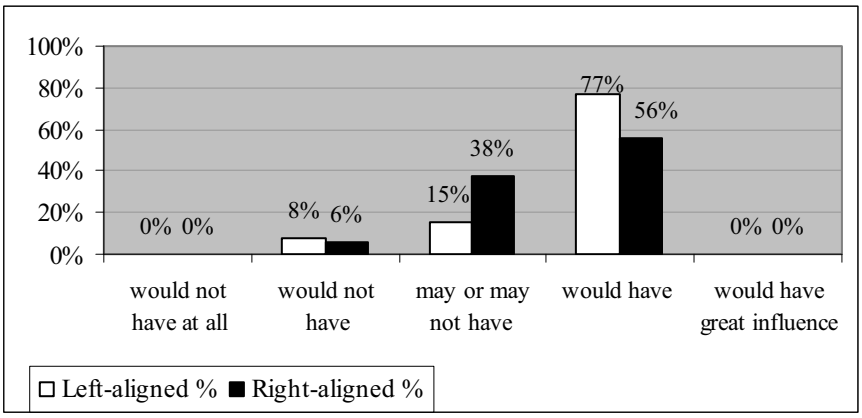

Figure 2: Citizens' e-participation influence on the quality of legislation and other decisions

Furthermore, the results show that there is a difference in Left/Right agreement with the statement "E-voting would contribute to a greater legitimacy of elected authority." Most of the right-aligned deputies (44%) disagree with this statement, while most of the leftists (46%) agree with it. On a scale of 1 to 5 the median for the Right is 2, while the median value of the Left is higher – 3.

The difference can also be seen after analysing the agreement with the statement "E-voting is secure" – most of the Right (50%) disagrees, while 42% of the Left agree and the same share neither agree nor disagree with this statement. On a scale of 1 to 5 the median of the Right is 2, and the median value of the Left is 3.

When it comes to the influence of e-voting on higher polling participation, the deputies are even more heterogeneous; most (50%) of the right-aligned deputies agree that e-voting would have influence on a higher turnout and most (85%) of the Left agree with this statement, too.

Most (69%) of the left-aligned deputies agree that e-voting would have influence on the movement in electoral body; on a scale of 1 to 5 the median of their agreement is 4. On the other side, most of the right-aligned members (44%) neither agree nor disagree with this statement; their agreement's median is 3.

If we neglect the Left and Right division and take a look at Figure 3, we can see that the situation is rather pessimistic. Most of the deputies (34%) disagree with the statement that e-voting would have an influence on the greater legitimacy of elected authority, only 28% of them agree and the same proportion (28%) neither agree nor disagree that e-voting is secure, while most of them (45%) agree with the statement "e-voting would have influence on the movement in electoral body."

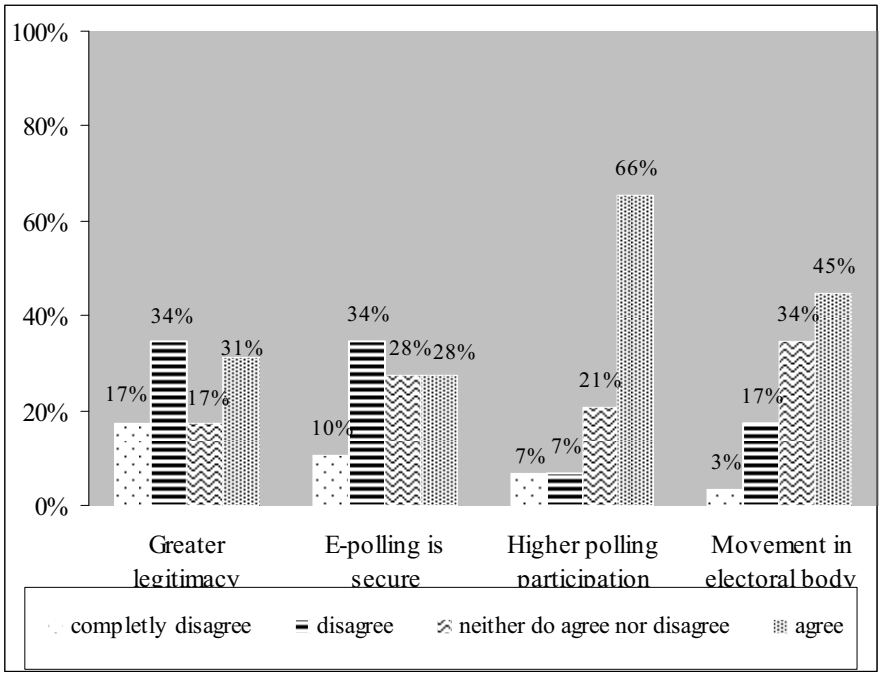

Figure 3: Deputies' views on e-voting effects[7]

There is one optimistic result – most of them (66%) agree that e-voting would have influence on higher polling participation (turnout).

[7] None of the representatives completely agreed with the statements listed above.

4.4 The reasons for Slovenia still not having a legislative basis for e-voting

We wanted to find out the main reasons for not having at least a legislative basis that would enable e-voting in Slovenia. The results[8] show that most (45%) of the deputies blame "underdeveloped" technology for the legislative "vacuum." Furthermore, 17% of deputies thought that the reason for not having a legal basis is the fear of some political parties that implementing e-voting would cause higher participation of younger and technologically more educated registered voters.

As may be seen from Figure 4, most (60%) of the right-aligned deputies blame the "underdeveloped" technology, while most (42%) of the left-aligned deputies blame the fear of some political parties, which are worried about higher turnout caused by e-voting.

Beside the reasons listed below (Figure 4), the respondents expressed some other reasons, such as (1) how would one assure that every voter had only one vote, (2) the risk that a voter could vote instead of other members of the family, (3) how to prevent people breaking into the e-voting system, (4) how to achieve voters' trust in e-voting, (5) bureaucratic reasons (formalities).

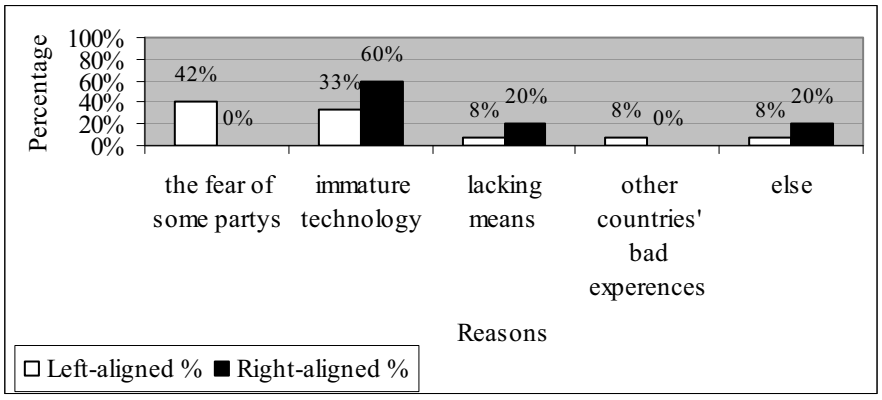

Figure 4: The reasons for not having a legal basis for e-voting

4.5 E-voting risks

We also asked the deputies which, in their opinion, are the greatest risks of e-voting. They were able to choose three answers at most.

[8] n = 27

The survey revealed that most of the respondents (66%) saw the biggest e-voting risk as the violation of some basic election principles: secrecy, freedom and (re)check. The lowest (24%) proportion of respondents was worried about double voting, and (28%) manipulation by the current ruling powers. Furthermore, 52% of deputies thought that excluding people who do not use the internet and those, who are not educated enough to e-vote is a threat to e-voting success, and 45% of them had doubts about system (collapse); 31% of deputies selected its possible influence on voter's decisions.

It is not surprising that, in contrast to the Right (13%), 46% of left-aligned deputies saw the main risk of e-voting as the possibility of manipulation by the current ruling powers.

5 The future of e-voting project in Slovenia

In this part we wanted to resolve two matters:

- to what level do the deputies support the implementation of e-voting (they were able to choose whichever level) and
- when, in their opinion, will Slovenia start testing e-voting.

The results show that most deputies (66%) support e-voting for national referendums, 48% of them support e-voting in the elections for president of the state, 48% support e-local referendums and 38% of respondents support e-elections of deputies. It is obvious that deputies are most sceptical about e-elections of themselves.

There is a significant difference in Left and Right support (Figure 5). As we can see, local e-referendums are supported by 69% of Left members, while only 31% of the Right members support this project. Moreover, 38% of Right members do not support any kind of e-voting, while all Left members support e-voting on at least some level listed.

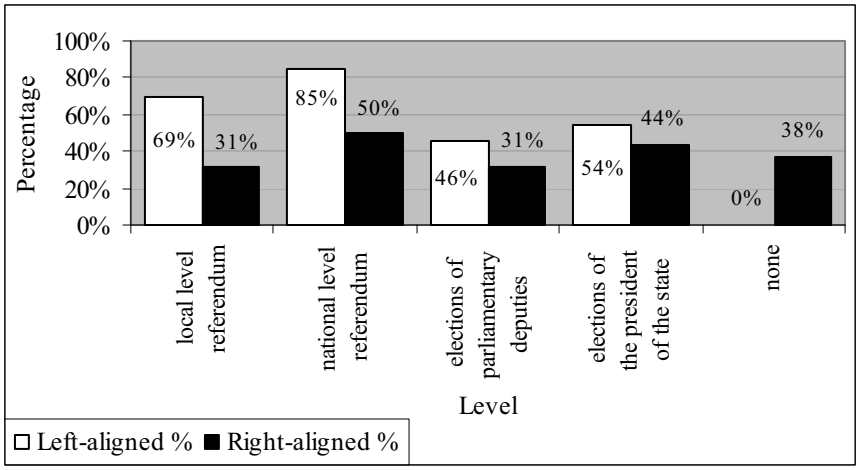

Figure 5: The levels on which Slovenian deputies support the implementation of e-voting

A total of 46%[9] of respondents thought that Slovenia will start e-voting test projects before 2010, among which were 62% of Left and 33% of right-aligned deputies, while 54% of respondents thought that e-voting projects would start after 2010 (38% of Left and 67% of Right).

5 Final remarks

The most interesting survey results can be summarized as follows:

- it is strange that only 14% of right-aligned members were well informed on other countries' e-voting projects, because the Right has been most responsible for delaying the amended law to enable e-voting. If they are not aware of others' countries e-voting projects in detail, than it is clear that their resistance to the amended Act was not based on professional arguments;

- some 48% of deputies thought that e-communication was only partly equivalent to traditional communication of proposals, initiatives, questions etc., but 85% of respondents said that they thoroughly study the initiatives etc., received via e-mail and take them into consideration as much as possible; on the other side, the survey [De05] revealed that deputies' response levels are not very high – 40% of them responded to a simple real case question from an imaginary citizen;

- the fact that 77% of the Left and only 56% of the right-aligned deputies thought that citizens' e-participation would influence the quality of legislation and other decisions is something to be anxious about, since the current ruling coalition consists primarily of right-aligned deputies;

- only 48% of respondents supported e-voting on the local level, which is interesting, since most of other countries started with e-voting projects on the local levels (municipalities); moreover, Rivest [html1] assesses, that local (county) level e-voting projects were more highly recommended than state e-voting (see section 2.1); it is possible that this answer is correlated to the forthcoming local elections in Slovenia; furthermore, it is interesting that the lowest proportion of respondents expressed support for the e-voting of deputies. If we look at these results critically, the message seems to be "e-vote for anyone, but not for us";

- some 21% of deputies neither agreed nor disagreed with the influence of e-voting on higher polling participation (turnout); this result is understandable, since the authors and other countries' experiences are not united on this question, either (see section 2.1);

[9] n = 28

- some 14% of deputies thought that lack of resources was the reason for not having at least a legislative normative basis for e-voting in Slovenia, which is, according to the findings of Remmert [Re04] and Van Den Besselaar et al. [VODF03] inexcusable, since e-voting could, over time, actually reduce costs (see section 2.1); some respondents saw the reason in the problems of ensuring the 'one voter – one vote' rule, which, according to Estonia, should not be a problem at all, since Estonia used multiple voting to reduce other people's influence on a voter's decision (see chapter 2.1)

It is evident that Slovenia cannot expect the implementation of e-voting in the near future. Our initial hypothesis was confirmed – the current ruling powers were not in favour of e-voting. Right-aligned deputies are much more sceptical about the implementation of e-voting than the left-aligned, which is something to be worried about, since the current ruling collation largely comprises right-aligned deputies.

References

[html1] Rivest, L. R.: Electronic Voting. Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, http://theory.lcs.mit.edu/%7Erivest/Rivest-ElectronicVoting.pdf.

[AP04] Arh, M., Peulič, D.: Profil volivcev posamezne stranke. Gfk Orange No 35, Gfk Gral-Iteo, October 2004, http://www.gfk.si/lnovice.php?NID=1139#.

[Ce05] Cerar, G.: Prezrti estonski zgledi. Mladina (44), October 2005, http://www.mladina.si/tednik/200544/clanek/uvo-manipulator--gregor_cerar/.

[De05] Dečman, M.: Responsiveness of E-Government and the Case of Slovenia. Proceedings of the 5th European Conference on e-Government, ECEG 2005 (Remenyi, D., ed.), University of Antwerp, Belgium 16-17 June 2005. Academic Conferences Limited, UK, 2005.

[GLZ04] Grad, F., Lukšič, A., Zagorc, S.: Ustavno-pravni in politološki vidiki uvajanja e-volitev v RS, Študija izvedljivosti, 2004 http://mid.gov.si/mid/mid.nsf/V/K2633A9BFD03509F2C1256E52005D938F/$file/Evolitve_ustavnopravni_in_politoloski_vidiki.pdf.

[ID03] IDABC. E-voting fails to raise electoral participation in the UK, says independent report, E-government news, 26 June, 2003, http://europa.eu.int/idabc/en/document/1431/358.

[IT04] I. T.: Ali bi bili pripravljeni voliti prek interneta? Delo, Informacijska tehnologija: 08.10.2004. In: Research of Internet in Slovenia, 29.10.2004, http://www.ris.org/main/novice/readnews.php?sid=137.

[Ko04] Kodelja, M.: E-paranoja države. January 2004, http://www.mojmikro.si/articles/60_61_e-volitve.pdf.

[MIS03] Ministry of Information Society: Zasnova študije izvedljivosti elektronskih volitev, Ljubljana, December 2003, http://mid.gov.si/mid/mid.nsf/V/KBF59760A55676EA3C1256E52005DAC22/$file/Evolitve_zasnova_studije_izvedljivosti.pdf.

[NEC04] The National Election Committee: General Description of the E-Voting System. Talinn, 2004, http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf.

[No02] Norris, P.: E-Voting as the Magic Ballot? The impact of Internet voting on turnout in European Parliamentary elections, Paper for the Workshop on 'E-voting and the European Parliamentary Elections' Robert Schuman Centre for Advanced Studies, Villa La Fonte, EUI 10-11th May 2002. http://ksghome.harvard.edu/~pnorris/ACROBAT/Magic%20Ballot.pdf

[Re04] Remmert, M.: Towards European Standards on Electronic Voting. In: Prosser A., Krimmer R. (Eds.): Electronic Voting in Europe − Technology, Law, Politics and Society, Austria, 2004, p. 13-16, http://static.twoday.net/evoting/files/E-Voting-in-Europe-Proceedings.pdf.

[So05] Site officiel de l'Etat de Geneve: Different views of evoting – The Geneva Internet Voting System, October 2005, http://www.geneve.ch/evoting/english/presentation_projet.asp#impact.

[SO06] Statistical Office of the Republic of Slovenia. Usage of information-communication technologies (ICT) in households and by individuals. Rapid Reports No 6/2006 – Information Society. Ljubljana, January 2006, http://www.stat.si/doc/statinf/29-SI-100-0601.pdf.

[Tu04] Turk, M.: Študija izvedljivosti e-volitev s predlogi implementacije, Ministry of Information Society, Ljubljana, February 2004, http://mid.gov.si/mid/mid.nsf/V/K7F5A0C562D52B67BC1256E53003C431B/$file/Evolitve_studija_izvedljivosti_mid.pdf.

[VODF03] Van Den Besselaar, P., Oostveen, A. M., De Cindio, F., Ferrazzi, D.: Experiments with e-voting technology, experiences and lessons. In: Cunningham, P. et al. (Eds.): Building the Knowledge Economy: Issues, Applications, Case Studies. IOS Press, 2003, http://www.social-informatics.net/Bologna2003.pdf.

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER - Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods - Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahnič (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 - Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement - Erfahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometric and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 - Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-86 Krimmer, R. (Ed.): Electronic Voting 2006

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14
53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de