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

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

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

The volumes are published in German or English.

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

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

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

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

P-47

GI-Edition

Lecture Notes in Informatics

Alexander Prosser, Robert Krimmer (Eds.)

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

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

Proceedings

Alexander Prosser, Robert Krimmer (Eds.)

Electronic Voting in Europe
Technology, Law, Politics and Society

Workshop of the ESF TED Programme
together with GI and OCG

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

Gesellschaft für Informatik 2004

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

Volume P-47

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

Volume Editors

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

Series Editorial Board

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

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

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

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

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

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

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

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

Vienna, July 2004 Alexander Prosser, Robert Krimmer

Programme Committee

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

Organizing Committee

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

Sponsors

European Science Foundation

Gesellschaft für Informatik

Austrian Computer Society (OCG)

Austrian Chamber of Commerce

Regional Government of Vorarlberg

Preface

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

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

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

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

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

Vienna, June 2004

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

Jürgen Weiss MP
President of the Austrian Federal Council

Content

Keynotes

Towards European Standards on Electronic Voting

Michael Remmert

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

E-Democracy in E-Austria

Christian Rupp

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Alexander Prosser, Robert Krimmer

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

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

1 Introduction

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

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

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

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

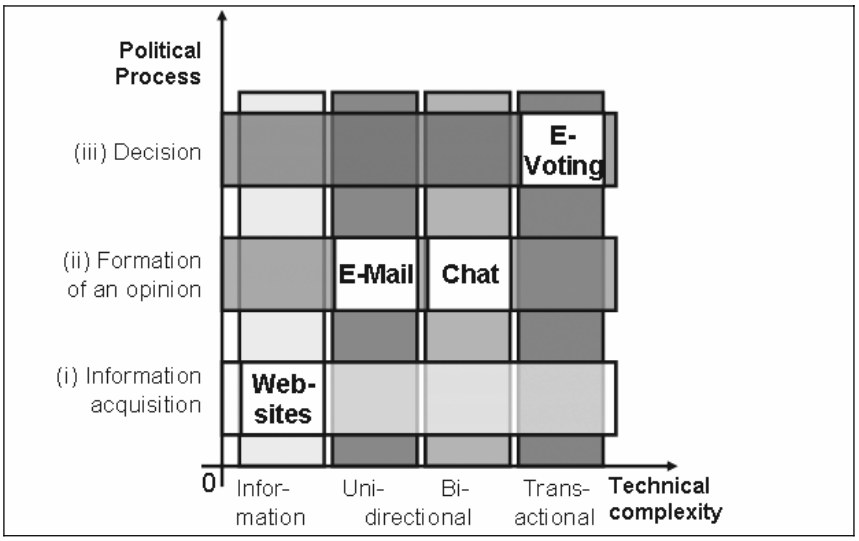


Figure 1: E-Democracy Application Framework

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

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

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

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

2 Existing Cross-National Research

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

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

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

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

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

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

Table 1: EU Forum Case study template

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

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

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

3 The Model

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

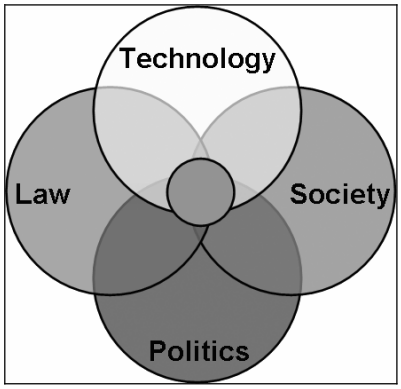


Figure 2: Dimensions of E-Voting

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

3.1 Dimensional Factors on the National Level

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

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

---

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

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

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

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

3.2 E-Voting Project Level

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

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

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

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

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

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

3.3 Assessment

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

4 Conclusions

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

5 Acknowledgements

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

References

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

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

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

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

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

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

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

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

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

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

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

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

Electronic Voting in Europe

E-Voting: International Developments and Lessons Learnt

Thomas M. Buchsbaum[1]

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

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

1 Growing attention to e-voting

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

2 An international overview

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 The Austrian case

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

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

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

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

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

[3] G18/85, VfSlg. 10.462

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

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

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

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

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

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

---

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

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

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

4 Council of Europe's standard-setting

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

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

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

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

---

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

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

5 Lessons learnt

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

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

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

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

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

---

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

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

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

6 How best to introduce e-voting

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

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

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

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

7 Conclusions

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

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

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

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nadja Braun

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

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

1 Introduction

1.1 Switzerland – a federalist state with direct democracy

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

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

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

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

2 Swiss e-voting considerations

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

2.1 Why is Switzerland considering e-voting?

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

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

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

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

2.2 The three pilot projects

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

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

2.2.1 Geneva: Three real e-votes[22]

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

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

---

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

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

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

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

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

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

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

---

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

2.3 Enhancement of voter turnout

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

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

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

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

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

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

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

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

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

3 Legal Framework

3.1 The legal provisions for the testing of e-voting

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

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

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

3.2 Secret suffrage

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

---

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

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

3.3 Free suffrage

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

---

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

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

4 The work of the Council of Europe

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

4.1 Legal standards

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

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

---

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

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

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

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

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

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

5 Conclusion: Recommendations to the Swiss legislator

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

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

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

References

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

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

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

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

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

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

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

Bernard Van Acker

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

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

1 Introduction

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

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

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

1.1. Definition

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

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

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

1.2. Contingency under current legislation.

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

1.3. Relevance for remote e-Voting schemes

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

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

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

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

---

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

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

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

2 The risk and the impact of voter coercion

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

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

A. the model.

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

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

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

We distinguish two kinds of players:

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

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

Throughout this description, we shall make the following assumptions:

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

---

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

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

We will now describe two scenarii.

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

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

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

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

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

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

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

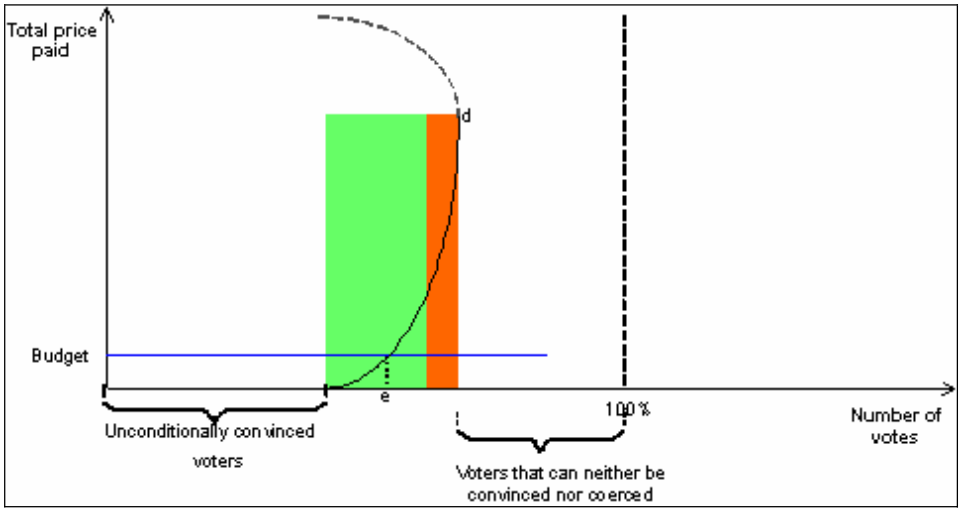


Figure 1: The total price of paying to get a certain result, versus a given budget (Swiss model).

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

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

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

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

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

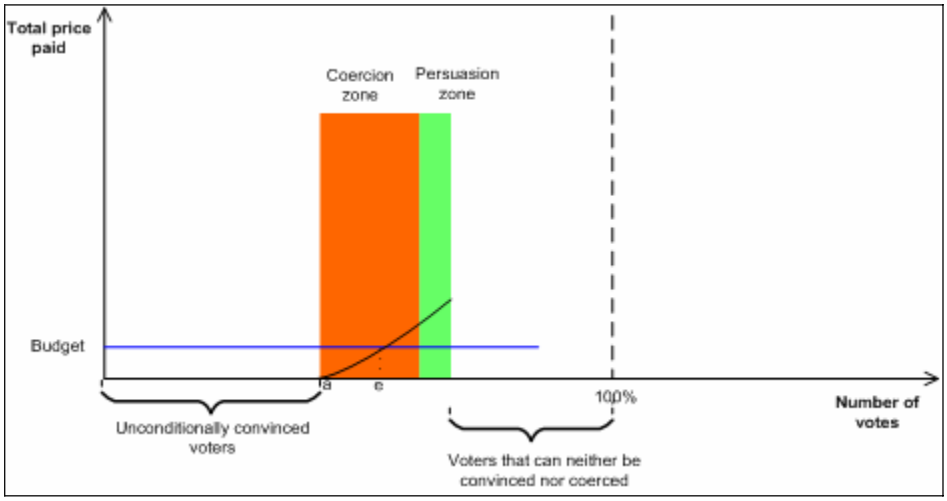


Figure 2: The total price to be paid for a certain result, versus a given budget (non-Swiss model).

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

B. Influencing Factors

B.1. Probability-influencing factors.

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

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

B.2. Impact-influencing factors.

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

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

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

a) The budget.

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

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

2.2. Practical risks with traditional voting methods

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

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

2.3. Practical risks with remote voting

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

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

3 Contingency against coercion.

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

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

---

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

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

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

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

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

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

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

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

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

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

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

---

[64] References are not exhaustive

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

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

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

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

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

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

4. Conclusion

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

E-Voting and Biometric Systems?

Sonja Hof

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

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

1 Introduction

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

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

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

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

2 E-Voting

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

3 E-Voting and Security

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

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

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

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

4 Biometric Identification in E-Voting

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Figure 2: FRR and FAR for three example biometric systems

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

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

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

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

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

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

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

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

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

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

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

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

5 Conclusions

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

Properties that have to be improved include:

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Anne-Marie Oostveen, Peter van den Besselaar

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

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

1. Introduction

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

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

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

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

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

2. Voter-verifiable electronic voting

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table 1: Trust in verifiability by other variables

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

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

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

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

4. Conclusions

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

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

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

5. Acknowledgements

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Towards remote e-voting: Estonian case

Epp Maaten

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

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

1 Introduction

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

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

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

2 Legislative basis

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

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

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

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

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

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

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

3 Basic principles of e-voting

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

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

---

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

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

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

3.1 Voters authentication with ID-card

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

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

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

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

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

3.2 Electronic re-vote and the priority of traditional voting

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

---

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

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

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

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

4 General concept of e-voting - the envelope method

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

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

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

The e-voting follows the same scheme:

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

The following figure illustrates the envelope method:

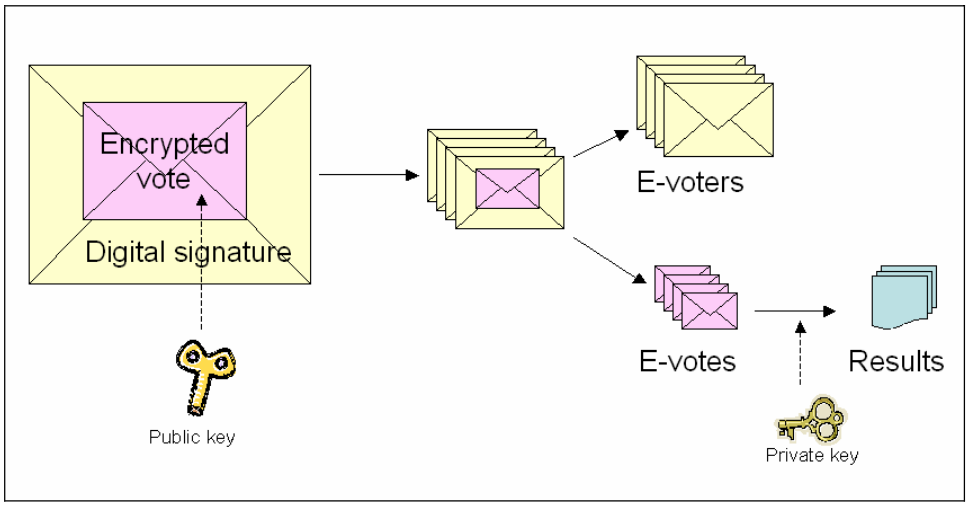


Fig 1: The envelope method [GD04; P 9]

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

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

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

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

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

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

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

5 Problems decelerating the implementation of e-voting

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

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

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

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

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

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

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

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

6 Current state of e-voting project and future plans

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

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

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

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

Literature used

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

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

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

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

Experimentation on Secure Internet Voting in Spain

Andreu Riera, Gerard Cervelló

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

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

1 Introduction

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

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

---

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

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

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

2 Pilot Objectives

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

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

3 Description of the Pilot

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

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

3.1 Creation and Distribution of the Voting Credentials

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

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

3.2 Pilot Promotion Campaign

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

3.3 Constitution of the Electoral Board

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

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

3.4 Vote Casting Procedure

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

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

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

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

3.5 Vote Tally and Verification of Results

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

4 Electoral Results

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

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

Table 1: Aggregated Results of the Pilot Vote

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

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

Table 2: Comparison of Postal Votes to Internet Votes

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

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

5 Voter Feedback

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

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

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

Table 3: Summary of Survey Results

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

6 Security risks and proposed solution

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

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

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

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

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

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

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

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

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

7 Concluding Remarks

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

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

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

Bibliography

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

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

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

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

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

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

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

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

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

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

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

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

Verifiability and Other Technical Requirements for Online Voting Systems

Niels Meißner, Volker Hartmann, Dieter Richter

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

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

1 Introduction

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

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

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

---

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

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

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

2 The catalogue of requirements

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

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

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

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

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

3 Selected Legal Questions

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

3.1 The role of an intermediate storage

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

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

3.2 The last call problem

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

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

3.3 Verifiability

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

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

4 Selected problem: Ensuring verifiability

4.1 Basic considerations

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

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

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

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

4.2 Principle applicable for systems using blind signature encryption type

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

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

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

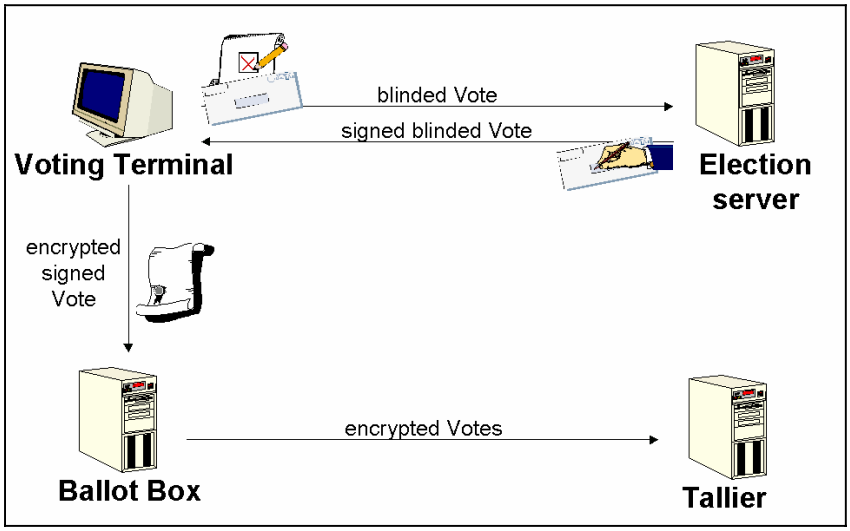


Figure 1: Schematic view of an Online Voting System using blind signatures

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

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

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

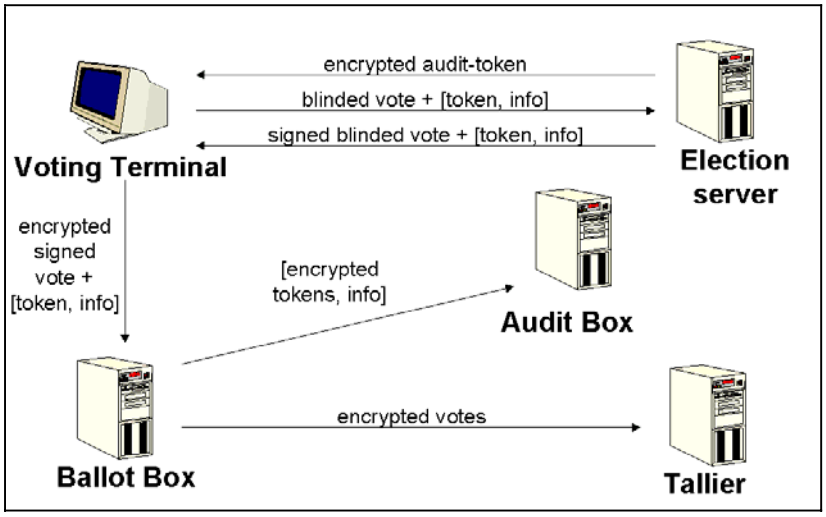


Figure 2: Schematic view of the audit data set approach

4.3 Principle applicable for systems using a homomorphic encryption type

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

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

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

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

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

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

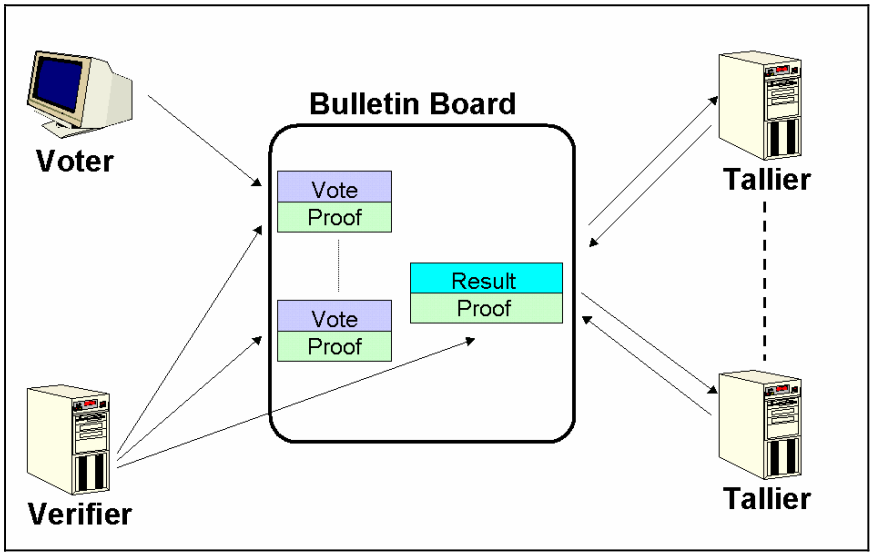


Figure 3: Schematic view of an online voting system using homomorphic encryption

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

5 Conclusions

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

From Legal Principles to an Internet Voting System

Melanie Volkamer, Dieter Hutter

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

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

1 Introduction

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

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

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

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

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

2 Legal Principles

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

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

3 Trust Model

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

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

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

3.1 Requirements to the system

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

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

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

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

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

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

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

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

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

3.2 Preconditions to the environment

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

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

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

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

4 Design

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

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

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

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

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

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

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

5 Realization

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

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

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

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

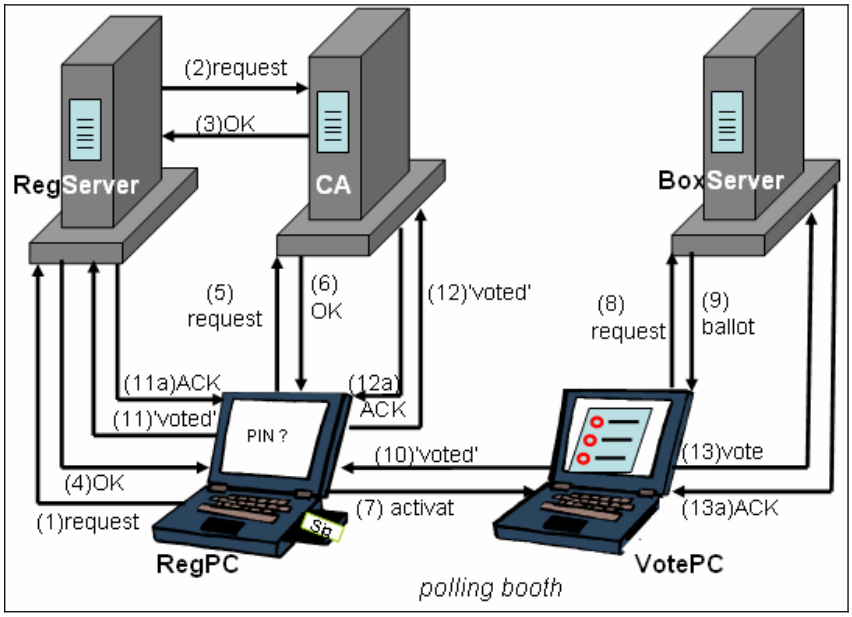


Figure 1: Architecture and Communication

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

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

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

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

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

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

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

---

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

6 Implementation

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

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

7 Related Works

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

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

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

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

8 Conclusion

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

Literaturverzeichnis

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

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

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

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

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

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

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

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

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

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

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

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

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

How Security Problems Can Compromise Remote Internet Voting Systems

Guido Schryen

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

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

1 Introduction

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

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

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

2 Security problems

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

2.1 Differences to e-Commerce

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

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

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

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

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

---

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

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

2.2 Assumptions and focus

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

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

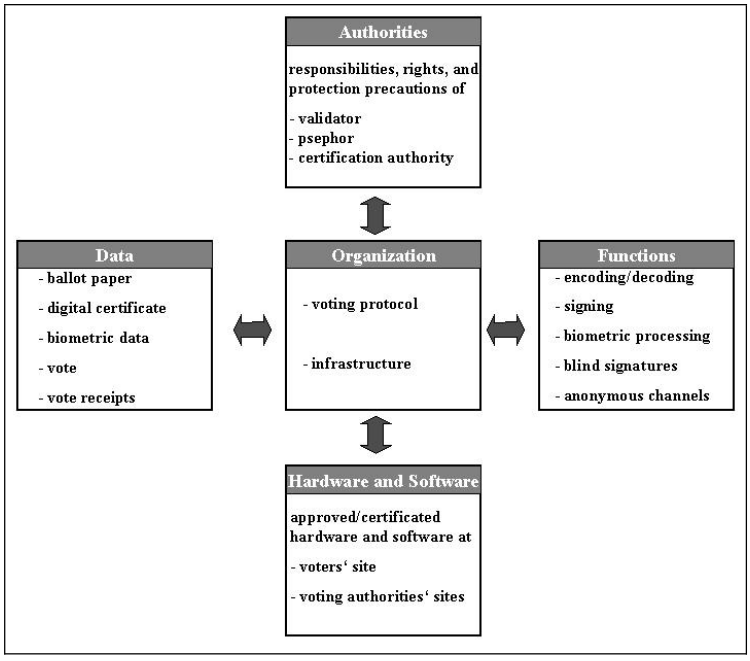


Figure 2: Security dimensions for voting systems [Sch04, p.7]

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

2.3 Client related security issues

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4 Server related security issues

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

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

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

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

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

2.5 Connection related security issues

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

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

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

---

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

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

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

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

3 Internet Voting Reports

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

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

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

3.1 CALTECH and MIT: Voting Technology Project

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

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

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

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

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

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

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

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

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

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

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

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

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

3.5 Research Group Internet Voting : i-vote

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

4 Conclusions

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

References

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

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

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

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

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

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

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

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

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

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

E-Voting and the architecture of virtual space

Anthoula Maidou, Hariton M. Polatoglou

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

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

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

1 Introduction

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

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

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

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

2 Method

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

2.1. e-voting environment: theoretical background

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

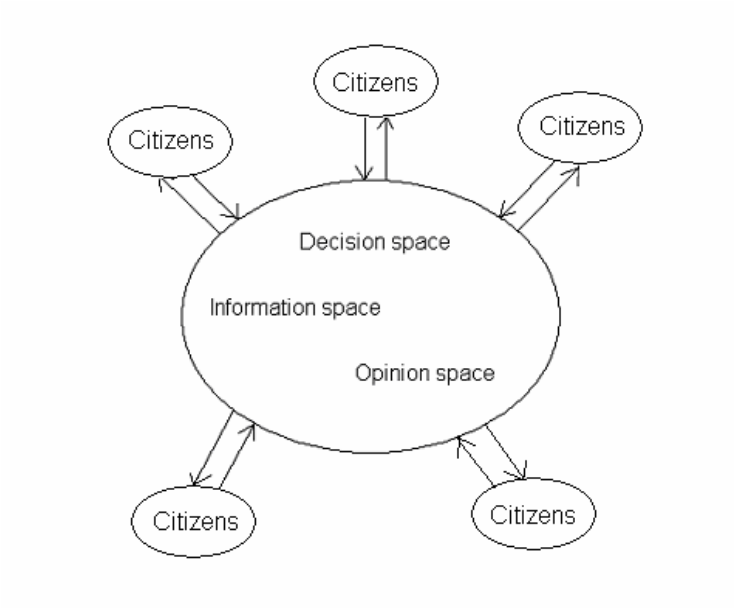


Figure 3: A many to many interaction of citizens with the decision process

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

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

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

2.3 Virtual space

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

The experience of a new kind of space isn't something novel. Since the implementation of the telegraph and later on the telephone and television, humankind is experiencing a new kind of perception, the "perception at a distance", or telesthesia [Mc94]. This experience is perceived as real, like the real world experience - it differs only in the fact that things are not bounded by the rules of proximity. Virtual space is also experienced as a real space - we use virtual space to get information on any subject, read the news, buy, visit libraries, museums, listen to music, etc. [Mi96]. Furthermore, the terms we use to refer to virtual space has a close analogy to the physical world: we talk about "virtual communities", "homepages" or "sites" that have "addresses", etc.

Virtual geographers study the geographies of the virtual space [DK01] using geographical metaphors. Additionally, we talk about the law of virtual space, protection of privacy, etc. Virtual space is perceived as a notional mechanism beyond the real world. Spatiality takes a new dimension; it can be electronically constructed and experienced. Through our memory we transform these experiences into possibly experienced realities. Virtual space is an extension of real space and can thus be analyzed in spatial terms.

2.2 E-voting interfaces

The main question we wanted to examine is how a successful human computer interface should be built, in order to attract people of various age groups, with a wide range of skills and abilities, and different degrees of voting experience, to take part at an election, or referendum. On the one hand we have special groups that are not familiar with the use of computers, and on the other we have the younger ages, which are familiar with computers, but show a minor interest in politics.

The question remains on how to communicate information, and how this information is correctly understood, in order for everyone to know what the voting is about, and also to give the impression of the importance this voting has. Originally, computers were designed by engineers for engineers – and little attention had to be paid to the interface. Later on, the use of computers by a broader, non-specialized user group necessitated the use of interfaces to enable them ease of use, correct understanding and interaction with the computer. The most important aspect in the Human Computer Interface design is to find efficient ways to design understandable electronic messages [No88, Sh98]. At this point we could take advantage of the achievements of virtual architecture.

In order to overcome these problems we propose that the appearance of the site should not be unique. As in electronic games, the visitors/citizens should be able to change the interface, choosing among various interfaces, in order to build their own environment, according to their taste. In this way people get familiarized with the voting environment.

A first step towards this direction should be the construction of more environments with various complexity and ease of use, which should be available to the visitor of the site, ranging from simple text sites, which should also be the default version of the site, to more complicate 3D graphics sites, to sites containing video and sound, or even navigable environments. At a second stage objects will be introduced, in a form similar to that of the avatars used in computer games, in order to invoke the feeling of their electronically projected self in this electronic environment, where interactions among the avatars (other visitors) could be possible. For example in the “Information Space” the various opinions could appear as avatars expressing their thoughts. A discussion group could also be organized as a place for the exchange of opinions. This could, in the future get the form of discussions among avatars. Such environments would specially invite the younger ages to take a look at the site, organize the interface according to their taste, get familiar with the structure of the site, and most important with the issue in question. In this way they will form an opinion, and probably take part at the e-voting process.

2.4 Virtual space

As to the interfaces and the navigation techniques, we used:

1.) A simple text and buttons interface in all spaces. Framed text displays the information, and links to the opinions, and the voting options. This is also the default interface.

2.) A 2d, or 3d graphics interface, which is used as a background. The actual interface remains about the same as in the first case.

3.) Video and interactive 3d graphics.

4.) Interactive navigable interfaces using VRML versions of the interfaces and graphical links.

3 Results

3.1 Presentation of some interfaces

Below we will give some examples. Because of the restricted space we will present only three interfaces. Of course, the acceptance of a virtual environment is not necessary – someone can also interact with the e-voting site using a default textual environment.

3.1.1 First example:

A scene reminding an ancient city market place serves as our first example. Picture 1 presents a part of it. In the center is a round temple, the tholos, with its altar formed as a multi-screen information place. It serves as the place, where information can be gained and also as the place for the exchange of opinions. Picture 2 shows a closer look at the information and opinion place. The upper section of the cylinder of the multi-screen contains the information space, while at the sides the opinions are displayed.

Picture 1: The first example displays an ancient marked (agora) interface. Here we present the part showing the "vouleftirion"(parliament) and the "tholos"(round temple).

Picture 2: The altar in the "Tholos" is a multiscreen projector. The altar plays the role of the information and opinion space.

Finally, at the voting date, the information and opinion space transforms into a voting-box, as presented in picture3.

Picture 3: At the e-voting day the altar transforms into a "kalpi" – a ballot-box.

3.1.2 Second example: a meeting room

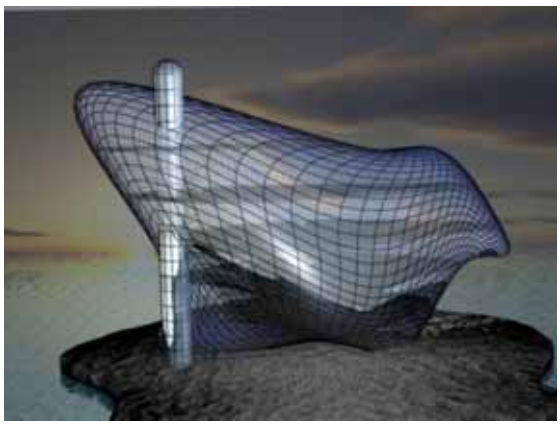
A large meeting table refers to discussion. The various opinions may be displayed as sheets of paper on the table, or as the human figures. Picture 4 presents such a room.

Picture 4: Second interface example, where the interface is a meeting room.

When it comes to voting the table transforms to a voting screen.

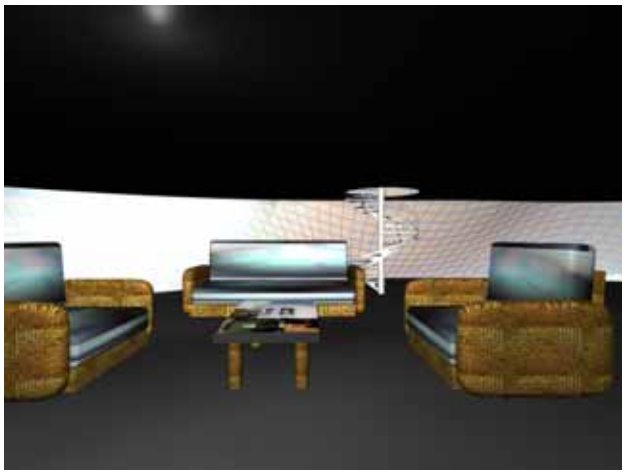
3.1.3 Third example:

Here the interface becomes an imaginary building, which refers to future environments.



Picture 5: The table of picture 1 transforms into an e-voting screen.

Someone enters the building and navigates in this VRML environment to gather information and express, read, or discuss opinions. An instance of how this could look is presented in picture 6.



Picture 6: An instance of the navigation in the information and opinion space

3.2 Testing results

We tested the interfaces on 16 persons, 9 women and 7 men, of various age groups1. With the help of a questionnaire, which was completed after the testing of the different interfaces, we found that both sexes and all age groups had no difficulty, at least after a short time they spend to get familiar with the interfaces. Some women and men of middle age group and all higher age groups participants preferred the simple text environment (about 35%) or the text and graphics interfaces (about 30%) and the video and graphics environment (about 35%), while the younger age groups were more attracted by the video and 3d graphics interface and the VRML navigate-able interface (about 50% for each).

In addition, more men (about 70%) were willing to spend more time reading different opinions, while a larger part of the women (about 65%) would prefer discussion groups.

Our findings showed that it is necessary to allow people to get familiar with the e-voting process through an earlier activation of the voting-site in the form of an information and opinion space.

---

[1] From the 9 women: 4 were under 30, 3 were between 30 and 55, and 2 over 55, while from the men 4 were under 30, 2 between 30 and 55, and 1 over 55.

Furthermore, about 60% of the younger age group admitted that they are in general not interested in politics and in community issues, but they would like to take part at e-voting processes, provided they could find objective information on the subject in question.

4 Conclusions

Current technological evolutions have changed the way we live, interact, communicate, learn, play get information, etc. Virtual reality techniques offer a new ground to architecture to take up expressing current knowledge and visualize data and information. The technological evolutions in accordance with the virtual reality techniques can be applied by governance in order to access the ideal of direct democracy. E-voting is the best way to allow citizens to express their opinion on major decisions of the political life of a community. Our findings showed that it is possible to attract younger voters, and encourage groups unfamiliar in the use of computers to participate.

References

[DK01] Dodge, M.; Kitchin R.: An Atlas of Cyberspace, Addison Wesley, 2001.

[KS03] Kampen, J.K.; Snijkers, K. : E-democracy - A critical evaluation of the ultimate e-dream. Social Science Computer Review. 21 (4): 491-496, 2003.

[Mc94] McKenzie, W.: Virtual Geography, Indiana University Press, 1994.

[Mi95] Mitchell, D.: The end of public space- Peoples Park, Definitions of the Public and Democracy, Annals of the Assosiation of American Geographers 85 (1): 108-133, 1995.

[Mi96] Mitchell, W.: City of Bits. MIT Press, 1996.

[No96] Novak M.: transArchitecture. 1996 http://www.mat.ucsb.edu/~marcos/Centrifuge_Site/MainFrameSet.html, as retrieved on 19.02.2004.

[No88] Norman, D.: The design of everyday things. New York: Doubleday, 1988.

[Sh98] Shneiderman, B.: Designing the user interface: Strategies for effective human-computer interaction (3rd ed.). Addison-Wesley Publishing, Reading, 1998.

[SM03] Smith, E.,; Macintosh, A.: E-voting: Powerful symbol of E-democracy. Electronic Government, Proceedings Lecture Notes in Computer Science, 2003, 2739: 240-245.

[TG03] Tambouris, E.,; Gorilas, S.: Evaluation of an e-democracy platform for European cities. Electronic Government, Proceedings Lecture Notes in Computer Science, 2003, 2739: 43-48.

[WC02] Watson, A,; Cordonnier, V.: Voting in the new millennium: eVoting holds the prondse to expand citizen choice, Electronic Government, Proceedings Lecture Notes in Computer Science, 2002, 2456: 234-239.

The UK deployment of the e-electoral register

Alexandros Xenakis and Prof. Ann Macintosh

International Teledemocracy Centre
Napier University
10, Colinton Rd,
EH10 5DT, Edinburgh, UNITED KINGDOM
a.xenakis@napier.ac.uk
a.macintosh@napier.ac.uk

Abstract: In this paper we analyse the experience gained in the 2002 and 2003 UK e-voting pilots in the implementation of the e-electoral register of voters. After theoretically establishing the need for an e-register, based on the analysis of the evaluation reports provided and direct observation undertaken in one of the pilots, we describe the systems used and identify the different organisational and technical issues that arose. Accordingly we highlight lessons learned, to be used for future implementations of the e-register.

1 Introduction

In August 2002 the UK government issued a consultation paper on a policy for electronic democracy [HM02]. This consultation document usefully argued that e-democracy could be divided into two distinct areas - one addressing e-participation and the other addressing e-voting. In the case of the latter the paper argues that e-voting should be viewed as a technological problem. In the case of the former, the document set out the possibilities for greater opportunity for consultation and dialogue between government and citizens. With regard to e-voting 16 pilots took place in May 2002 [Pr02] and 18 more in May 2003 [El03a], on a Local Authority level. These were in all cases legally binding elections. The different e-voting technologies piloted involved electronic counting schemes (in some cases combined with traditional paper ballots) touch-screen voting kiosks, internet voting, phone (touch tone) voting and SMS text message voting in 2002 [Pr02]. Digital television voting and smart card technology for partial voter identification were additionally introduced in 2003 [El03a]. Several local authorities (4 in 2002 and 13 in 2003) offered these technologies as alternative channels of voting, therefore providing a multiple channel e-voting process. In the pilots where two or more channels of voting were offered simultaneously an electronic on-line version of the electoral register was developed and used to provide the necessary infrastructure. The on-line electoral register was piloted in Liverpool and Sheffield in 2002, [El02a & 02b] and in Sheffield and St Albans in 2003 [El03b & 03c]. The focus of this paper is the analysis of the deployment and use of the e-electoral register.

2 Research methodology

The research presented in this paper forms part of a doctoral programme concerned with the identification of the emerging constraints in re-designing the electoral process in relation to ICTs. After completing an extensive literature review of the issues involved in the implementation of electronic voting, we have proceeded to the analysis of the detailed evaluation reports of the 2002 and 2003 UK e-voting pilots, provided by the Electoral Commission. Further research data have been provided directly by some of the 2003 pilot Local Authorities. Our research findings reported here on the e-electoral register are based on its use in one of the 2003 pilots. The Local Authority studied was piloting an on-line system of the electoral register, to support a simultaneous multiple channel e-voting process combined to provide e-enabled polling station voting. The fieldwork which comprised interviews and observations, was conducted both during the run-up to the election and on the actual polling day. Semi-structured interviews with Local Authority and commercial suppliers' staff were undertaken on the first day, during which, there were interruptions to allow for managerial problems to be resolved. In such cases the observer was allowed to follow the e-voting management in action. On election day, observation took place at the operations management centre, which was set up to handle the technical and organisational issues that arose. After 9pm that day, when voting was over, the observer was part of the verification processing team. That in turn provided the opportunity to acquire hands on experience of the administration of the e-register system used.

3 The need for the e-register of electors

The Electoral Commission in a report specific to the electoral registration process [El03d, p:18] recommends: "Electoral registers should be universally electronically maintained according to mandatory national data standards". It also refers to issues concerning registration fraud and measures that could be taken to prevent against such fraud. In the previously mentioned UK Government consultation paper, a system described as: "a local or national electronic electoral roll" p43 is suggested as necessary infrastructure for voting at any polling station. Also, the on-line electoral register is considered to be one of the major components of a modern e-voting system, along with "on-line registration and application for postal votes, on-line and text voting, e-counting and collating of election results" p45. The major benefit given for a central electronic electoral register is that election officials could authenticate a voter at any polling station. Research in this area has been undertaken by the LASER (http://www.idea-infoage.gov.uk/services/laser/index.shtml) project aiming at the production of a fully interactive online register. The need for the e-electoral register serves the basic security requirements that "only people who are entitled to vote can vote" and "nobody can vote twice or in another person's name (unless an authorized proxy)" [HM02, p46].

From a legal point of view voter identification is necessary in order to avoid personation [Xe03]. The Watt [Wa02] report defines the different cases of personation, while making the case for the legal requirement of 'one ballot per vote' and a verifiable count.

Furthermore, who is included in the electoral register is directly related to the issue of voter eligibility [OS01]. In accordance with the above, the statement of requirements for the design of the e-voting systems to be used in the 2003 pilots included a "Compliance with Legislation" term [OD02]. Technical security standards were also set according to CESG security solution [Cr02]. Managerial issues were also covered in the 2003 statement of requirements, including data management, risk management and staff training. The same set of requirements had a separate section for the electoral roll with several detailed functions that had to be developed by the suppliers and provided to Local Authorities. The most relevant functions with regard to this paper covered the necessity to convert any electoral roll into a format which is suitable for use in the pilots, immediately mark an elector as having voted as soon as the ballot is counted, provide upon request a daily marked register and allow a live continually updated register to be accessed remotely by the Returning Officer or the Local Authority staff.

4 Issues in the 2002 pilots

In the Sheffield 2002 pilot [El02b] three e-voting channels were simultaneously offered (internet, SMS text and kiosk voting) for a period of 6 days leading up to election day, along with voting in polling stations on election day. The existence of the on-line e-register enabled voters to cast a ballot at any polling station within their ward. Three wards out of twenty-nine were participating in the pilot. The voting channels provided in the Liverpool 2002 [El02a] pilot were similar to the Sheffield pilot with the only difference being providing telephone voting instead of kiosk voting. These were offered for the same period of time but only in two wards out of thirty-three. The e-register used a VRN (voter reference number) as a unique elector identifier, which was consumed once an e-channel had been used. That excluded double voting between e-channels. On election day a voter who requested a ballot from a polling station, was checked against the on-line e-register during the identification process. That excluded the possibility of a voter having already voted at another polling station or doing so later in the day. Polling officials by marking the e-register when giving a ballot would automatically consume the e-credentials of the voter and exclude the possibility of double voting between polling stations and e-channels. If a voter had previously applied for a postal vote then their e-credentials would also be consumed. In Sheffield a voter could go to any polling station of the participating wards and tell their name to the polling official. The polling official would in turn look the voter's VRN on a paper-printed list and input in the e-register interface. This made the process more time consuming than the traditional crossing off on the paper register. In Liverpool the same process was followed, but as an extra element of procedural security, voters were also crossed off a paper version of the register as would be done in the traditional voting process. This made the authentication process even more time consuming, about thirty seconds per voter, instead of five seconds needed had the traditional process being used. This, in turn, resulted in long queues building up during the evening.

4.1 Organisational Issues

A consortium made out of two commercial e-voting providers delivered both pilots. In Liverpool however a third commercial provider was involved in supporting the pilot effort (voter call centre). In Sheffield two PA departments were involved in the project (election office and IT) while in Liverpool four PA departments were involved (election office, e-government, marketing, press office), with the traditional voting channel managed separately. In both cases the project was lead by the main commercial supplier and there was a great amount of trust and dependence of the PA on the commercial suppliers due to time constrains in delivering the project. Risk management was adopted based on thirteen high-level risks, which were eventually detailed in late April –the election day was 2nd May. The 2002 risk tables were not provided in the 2002 evaluation reports. Polling station staff training was limited; in Sheffield one hour in the use of the register was provided prior to election day along with an instruction manual. In Liverpool two hours of un-paid training were provided but there was no time for process simulation. Limited staff training was considered to be an additional reason, which caused delays in the authentication process and also the reason for some of the technical problems encountered.

4.2 Technical Issues

Laptops and ISDN lines were used to connect polling stations to the on-line e-register. In Sheffield, there were also some cases of polling staff having difficulties in setting up the laptops, however a help-line provided assistance to polling station staff. Overall, only 4 cases were reported of voters being denied the right to a ballot as the e-register recorded them as having already voted. All these cases were attributed to processing errors. To cover the risk of hardware failure, contingency plans included one technician with a spare laptop per ward on polling day. To cover the risk of temporary system failure, provisions for keeping paper records of those who had voted at polling stations were taken for later entry once the system was restored. If the system was however permanently down then provisions were taken to convert immediately to traditional elections without the option of voting at any polling station. In Liverpool similar contingency planning was in place. ISDN connection problems were reported in two cases and were attributed to poor staff training; apparently polling station staff had damaged the equipment provided in their effort to install it. Technical support was provided to rectify the problems with backup hardware. In another case, a polling station received the wrong laptop. The polling clerk did not follow the agreed contingency procedure (telephone the central office and verify the eligibility of each elector) and for two hours issued ballot papers keeping manual notes of the voters who had been given a ballot only to update the database once the problem had been restored. Although all voters were later proved to have been eligible for the ballot they had received, there was a clear possibility for them to double vote during that time through another voting channel. The 2002 Liverpool pilot indicated that human errors could lead to technical risks and procedural disruptions. Had the lesson been learned for this case, problems might have been prevented in the 2003 pilots involving the use of the e-register.

5 Issues in the 2003 pilots

In the May 2003 elections St Albans [El03c] provided a multiple channel e-voting process including touch-tone telephone, kiosk and internet voting for a period of three days leading up to election day, along with simultaneous voting in polling stations on election day. The existence of the online e-register enabled voters to cast a ballot at any polling station as all twenty wards and twelve parishes were involved in the pilot. Additionally SMS text voting was offered in Sheffield [El03b], along with smart cards, which were used to facilitate the authentication process at polling stations and kiosks. The Sheffield 2003 pilot lasted for a voting period of seven days, with election day being the last one, however only fifteen out of twenty-nine wards participated in the pilots. The e-register system used in both pilots was the same as the commercial supplier provided it. The system provided seven functions: voter search, marking the register, credential management authentication, issue of replacement credentials, issue of tender credentials, checking the contest history of a voter and viewing an audit log for each voter.

In both cases laptops were necessary in order to maintain and update the electronic version of the electoral register in real-time from each polling station. This was necessary to avoid double voting as any voter could, up to the last moment (9pm on election day), cast a ballot through any of the voting channels offered. In practical terms this means that if a voter cast a ballot via a kiosk and then attempted to vote in person at a polling station the polling official equipped with a laptop connected to the database of electors (e-register) through the internet, would know that this voter had already cast a ballot and would subsequently deny a second ballot to this voter. More importantly, as voters were offered the option of voting at any polling station in all wards experimenting with the use of the electoral register on election day, the updated e-register would prevent a voter from voting at more than one polling station.

In Sheffield laptops were also used in polling stations to introduce an innovation at the authentication process. Each laptop was connected to an external smart card reader and voters were provided with the option of bringing their smart card to the polling station. The smart card could be used by the voter in front of the polling official and once passed over the smart card reader (non-contact smart card technology was used) the voter's details would automatically be recalled from the on-line e-register. The polling official would then ask the voter their name and address to verify against the screen information from the e-register database, and in this way complete the authentication of the voter. This should have been a 10 seconds process for each voter. The aim of the smart card was therefore to produce time efficiency in the polling station voting process. The smart card's memory element contained the voter identification number. It could also be used in kiosks. Once inserted in the smart card reader of the kiosk the voter ID would appear on the screen and voters would only have to supply the system with their password. However in all cases the use of the smart card was optional. At a polling station a voter could just walk in, state one's name and address, then the polling official, using function one, enter these details and authenticate the voter looking at the e-version of the register rather than the paper version of the register.

This was supposed to be a 30 seconds process and such was the case in St Albans where no smart card was introduced. Similarly at a kiosk a voter could type in one's voter ID instead of inserting one's card in the smart card reader. In all cases the smart card did not contribute any extra element of security but was rather provided as a means of convenience.

5.1 Organisational issues

A total of eight commercial suppliers had to work together to provide the Sheffield pilot [El03b], while the PA contributed with the election office, and staff from the IT department and the office of the Returning Officer. In St Albans [El03c] seven commercial suppliers were involved and the PA contributed with the IT department and a dedicated e-voting working party. Commercial suppliers were either directly contracted or subcontracted by the main providers. The main suppliers were the same for both Local Authorities.

Following basic IS project management principles [Av03] one would expect contingency planning at least equivalent to the one identified in the 2002 pilots. The statement of requirements for the 2003 pilots [OD02] asked for the implementation of a methodology compatible with PRINCE2 [Be02]. St Albans PA did provide an approach consistent with PRINCE2 while Sheffield PA followed its own methodology. In both cases risks were managed as they arose. However the matter of reliance of the PA to commercial suppliers for the safe delivery of the pilot remained and was characterised as over-reliance by independent evaluators working for the ODPM [El03b].

With regard to polling station staff training, the evaluation reports indicate that a greater effort was undertaken than the previous year. St Albans provided a detailed training programme, while Sheffield provided a two-hour walkthrough of the system for at least two out of three polling clerks of each polling station. However trainees were not given the opportunity to browse the system prior to election day, and gain familiarity with the different features. Instead they were provided with and interactive CD and a detailed manual. For Sheffield in particular no training was provided on the connection of the smart card reader to the laptop.

The organisational problems that arose were similar in both pilots. In Sheffield [El03b], there were delays in the delivery of laptops and smart card readers, while the number of back-up systems proved to be insufficient. Laptops were incorrectly configured by the responsible subcontractor, who also provided half the promised technical support staff with no transport and no knowledge of the area. Polling stations were not provided with a back-up paper copy of the register, as was the case in the previous year. In St Albans [El03c], the hardware required at polling stations on the morning of election day, was installed but not operational (41%), delivered but not installed (43%), or in very few cases not even delivered (5%). According to the project plan polling stations would be equipped with the necessary hardware the day before election day or even very early in the morning of election day (5am-8am). The reason was the unavailability of dedicated locations to serve as polling stations, which posed time constraints as to when the installation could take place. The time and the resources needed to set up polling stations

were underestimated. Inadequate logistical planning resulted in engineers being sent to polling stations without local maps and site installation diagrams. In both cases there was concern about the internal communication between the main contactors and their subcontractors.

Organisational problems, along with the technical problems described in the following section, resulted in a significant number of polling stations not being connected to the e-register in the morning of election day. In Sheffield the back-up procedure was that polling officials would call the election office and the election office staff would enter the voter in the e-register. However election office staff was unavailable and hand written notes were kept by polling clerks on those voters who had been given a ballot. There was also a written instruction given out to polling officials asking them only to give a ballot paper to a voter when marked on the e- register and not before and if in doubt contact the election office. Following instructions some polling officials did not give out ballot papers and some voters were sent away advised to come back at a later time in the day or use an alternative voting channel. According to the Electoral Commission this resulted to 200 voters being sent away [El03b].

In Sheffield, the main source of confusion in managing problems derived from the fact that there was no provision for established channels of communication between the polling stations and the election office. In St Albans mobile phones were issued to polling station officials. Sheffield on the other hand relied on the provision of telephone lines at polling stations.

The solution suggested, to provide election officers with a paper copy of the register, would have to be a copy of all registered voters in all participating 15 wards. If such copies were not already available, they would have to be printed out and then delivered to the polling stations facing problems in the use of the electronic form of the register. The copy of the register provided to the polling stations in question would be marked with the voters who had already cast a ballot through a different voting channel during the previous days. Although this measure would not provide total security against possible election fraud, as voters could vote again and again at polling stations where there would be no form of real-time updated register, it would limit the possibility of fraud, as it would exclude those who had already voted from voting again. However, the suggested solution was not feasible because of the large number of polling stations reporting problems with the e-register. In contrast, St Albans did provide the polling stations facing problems with the e-register with marked paper copies of the electoral register early on election day [El03c], but these reflected the status of the register at one particular time (10.15am) and were not subsequently renewed later in the day.

In relation to the voting process, when smart card readers did work, then the process could also be delayed instead of expedited as expected. Voters did not know how to use the card because there was no voter education on that matter. The smart card used in Sheffield was of the latest technology and in effect that was the problem as the technology was so new that people had no user experience of it. It was a “proximity card”. A voter did not have to insert it in a slot, as would have been the case in using a kiosk or any automated cash dispenser. In effect the card was contact less and it had to

be passed slowly over the smart card reader. Typically voters would put the card on the reader or pass it over quickly and the reader would not recognise the voter ID contained in the card. More efforts were needed to get it right and as a result more time. The problem could have been limited had training on the use of the card been provided to the polling officials, who could then help voters effectively.

At the close of polls, all the polling stations, which had kept manual notes on the voters who had voted without being properly authenticated, returned these notes to the election office. Normally the notes would have the name, surname and street address of each voter. The verification process started at 9pm after the e-voting channels closed. The database would then be searched usually with one term (surname) and accordingly verified on screen in relevance to the rest of the data. If the voter was shown as not having voted then he/she would be marked and there was no problem. If the voter was shown as having already voted there were available audit trails providing information as to the channel this voter had used.

However this was a time critical procedure because the result could not be announced before this process was over and the possible damage done during the day (double voting) fully measured. There was no consistency in the form of notes provided by different polling stations. All of the notes were hand written which in some cases caused confusion as to what was written. The objective of the verification process was to check and mark the register as should have been done during the authentication process prior to granting a ballot. If the register were already marked that would mean that a vote had already been cast on an e-channel and that the paper vote should be counted as valid. The general rule in the multiple channel voting was that if double voting had indeed happened then the e-ballot would be ignored and the physical (paper) ballot counted. This rule would cover the case where someone had voted twice, once in a polling station and once in any of the e-channels. However the case of a voter casting a ballot in two or more polling station was not covered, as all these ballots would be paper ballots. The process followed is an example of a procedural security measure [Xe04] adopted to cover for a technical inefficiency.

5.2 Technical issues

Regarding internet connectivity, in some cases the e-register, would respond more slowly than expected. This could be attributed to any number of different reasons, for example, the database server being overloaded (performance degradation). In such cases manual notes were kept to enter later when the system performance allowed it. That mainly caused periodic crashes around the end of the day and it was attributed to data indexing problems at the bottleneck of the back-end application. ISP poor performance also resulted in a slower process by not transporting data at the expected internet speed. ISPs guarantee connection to the internet but not internet performance. Dedicated fixed connections or the use of an owned ISP was suggested as a future, nevertheless more expensive, solution.

Connectivity problems also included some polling stations loosing their connection from time to time. In cases where there were long periods of time between two voters coming to be identified the connection would automatically drop. This lack of continuous connectivity meant that polling officials would have to re-log on to the database when the next voter needed to be authenticated. On entering the database for the first time polling officials were prompted to change their password. In one similar case the polling official forgot the new password that he/she had provided and therefore could no longer gain access to the e-register.

In Sheffield, hardware problems were also reported in relation to the smart card readers. The smart card readers were an external element linked to the laptops with a cable connection but they had a different power supply, which proved fragile. Polling station staff had to take the laptop and the smart card reader out of their cases, place them on a table, link them in the appropriate way according to each different laptop make, and then plug-in both power supplies and start the computer. The problem was not the reader itself but the separate power supply provided for the readers. Nevertheless a defective smart card reader did not stop a polling station from accessing the on-line e-register, but only changed the way voter searches were done.

Finally, with regard to the risk of power cuts, which was discussed at length in the 2002 Electoral Commission evaluation reports, the use of UPS units was reported only in St Albans. Nevertheless, normally charged laptop batteries could have kept the polling station operational for about four hours.

6 Conclusions

An e-enabled election is made more difficult to deliver as the scalability of the project increases. The deployment of the e-register studied in this paper, highlights the following issues:

- There is a need to establish standard communication channels between all the agents involved in the delivery and management of the e-register. The provision of alternative networks of communication such as the use of mobiles in St Albans proved useful practice, which facilitate the management of the problems faced and the need for feedback and problem escalation mechanisms between the agents related in the delivery of the pilot.
- There is an obvious need for a co-ordinating agent when many different agents are involved in delivering intersecting e-voting processes.
- The type and quality of internet connection used and the well-organised technical support provided, will determine the time needed to authenticate voters.
- Backup procedures such as a paper version of the register must remain available before problems arise, at least until the new process is well established.

- Systematic staff training in the new methods of voting to a level of being able to provide on-sight voter education and process knowledge gathering can provide valuable input to future best practice.
- Problems in e-enabled voting, resulting in process risks are related to the one-off use of voting locations (polling station) for the purpose of voting and every extra piece of equipment used.

From a more generic point of view, loosing voters who would have voted if not prevented by malfunctions in the e-enabled electoral process, could become a major political issue when affecting larger number of voters. This fact could in turn undermine the validity of the result of the electoral process as a whole, even if only one of the voting channels were problematic. The lessons learned from the deployment of the e-register in the UK can serve as a set of valuable guidelines for the future design and deployment of e-voting systems.

References

[Av03] Avison, D.E. & Fitzgerald. G., Information Systems Development: Methodologies, Techniques and Tools, 3rd Edition, McGraw-Hill, Berkshire, (2003)

[Be02] Bentley, C., PRINCE2: A Practical Handbook, Butterworth-Heinemann, Oxford, (2002)

[El02a] Electoral Commission. Pilot scheme evaluation Liverpool City Council 2 May 2002

[El02b] Electoral Commission. Pilot scheme evaluation Sheffield City Council 2 May 2002

[El03a] Electoral Commission. Local electoral pilot schemes 2003, Briefing, April 2003

[El03b] Electoral Commission. Pilot scheme evaluation Sheffield City Council 1May 2003

[El03c] Electoral Commission. Pilot scheme evaluation St Albans City and District Council 1May 2003

[El03d] Electoral Commission, The electoral registration process, Report and recommendations, June 2003

[El03e] Electoral Commission. (2003e), Technical Report on the May 2003 Pilots

[HM02] HM Government. In the Service of Democracy - a consultation paper on a policy for electronic democracy. Published by the Office of the e-Envoy, Cabinet Office, London, (2002).

[OD02] ODPM, Electoral Modernisation Pilots, Statement of requirements, (2002)

[OS01] OSCE, Office for Democratic Institutions and Human Rights, Guidelines for reviewing a legal framework for elections, Warsaw, (2001)

[Pr02] Pratchett, L. " The implementation of electronic voting in the UK " LGA Publications, the Local Government Association, (2002)

[Cr02] The Crown, E-voting security study (2002)

[Wa02] Watt, B., Implementing Electronic Voting, A report addressing the legal issues by the implementation of electronic voting, University of Essex, (2002)

[Xe03] Xenakis, A. & Macintosh, A, A Taxonomy of Legal Accountabilities in the UK e-voting pilots. In proceedings of DEXA, E-GOV 2003, Springer, (2003)

[Xe04] Xenakis, A. and Macintosh. A., Procedural security in electronic voting, in the proceedings of the 37th Hawaii International Conference on System Sciences (HICSS 37), (2004)

Transparency and e-Voting
Democratic vs. commercial interests

Margaret McGaley, Joe McCarthy

NUI Maynooth
Computer Science Department
Co. Kildare, IRELAND
mmcgaley@cs.may.ie

Arkaon Limited
Sandymount
Dublin 4, IRELAND
joe.mccarthy@arkaon.com

Abstract: Electronic voting systems are being introduced, and have been introduced, in many countries for a variety of reasons. The introduction of computers into the electoral process can offer several advantages. Among other things it can speed up the process of calculating results, can help voters avoid accidentally spoiling their vote, and can allow voters with special needs to vote in private. Often, however, little consideration is given to the potential negative effects of electronic voting. We examine some of these negative effects in terms of the three streams of this conference: technology, law, and politics, with particular emphasis on the situation in the Republic of Ireland. The over-arching theme of this paper is that the introduction of technology into the democratic process can reduce transparency, and risks private commercial interests being given priority over public democratic interests.

1 Technology

The introduction of technology is often seen as necessary to progress, and therefore in some way unstoppable. All too often, however, little consideration is given to the new challenges - legal, political and sociological - posed by technology.

1.1 Transparency

Perhaps the greatest strength of paper voting systems is their transparency. Individual voters can satisfy themselves that the system works, because its transparency allows them to observe and understand every aspect of it. Nothing within the system is secret or impenetrable, except of course who casts which vote.

Purely electronic systems cannot offer this transparency. The nature of computers is that their inner workings are secret. Since transactions and calculations happen at an

electronic level, it is not physically possible for humans to observe exactly what a computer is doing. Once the vote is cast the voter "loses sight" of it. So if - for whatever reason - the vote is stored incorrectly, there may be no sign that something went wrong.

The change from paper to electronic records is not simply a matter of changing the storage medium. It is much more fundamental: the introduction of a computer system between voter and vote denies the voter tangible evidence that his vote has been recorded correctly. This is different from the paper system. While the voter never received evidence that he could take home, he did see the actual record of his vote (the paper ballot). Armed with the knowledge that pencil lead does not fade overnight, he could then be sure that the vote cast would be the vote counted. When the primary record of one's vote is electronic, on the other hand, one only ever sees a representation of one's vote, never the vote itself.

It is unacceptable that a voter should have to trust any agent or device to correctly relate their vote to them. Unfortunately, this is necessarily the case with purely electronic systems.

1.2 Voter Verified Paper Ballots

There is growing support worldwide [U.S, Sch00, Soc04] for the idea that 'Voter Verified Paper Ballots' (VVPBs [Mer92], also known as a 'Voter Verified Audit Trail') must be a requirement for electronic voting systems. VVPBs are paper records of the vote which have been verified by the voter at the time of casting. They might be hand-written ballots which are scanned for computer counting, or they might be printed by DRE (Direct Recording Electronic) machines in front of the voter before being deposited into a sealed ballot box [Mer02]. These paper ballots, however they were produced, would be the primary record of votes cast, since they would be the records verified by the voter. They would be used for all recounts and in a number of randomly chosen constituencies every time the system was used.

Some manufacturers of electronic voting systems, including the Nedap system being introduced in Ireland, have suggested that printing all the ballots after the close of polls would provide an equivalent audit trail. In fact this would be completely inadequate. The value added by VVPBs is that they are a record that has been confirmed correct by individual voters. If, by accident or design, the electronic records were incorrect then printed copies of those records would contain the same errors. As the old computer phrase goes - garbage in, garbage out.

Several paperless alternatives are under development [Cha04, JRB03]. However, we have yet to be convinced that any such system can provide the transparency necessary, or release voters from having to trust vendors.

The elimination of paper from elections is a significant motivating factor in the introduction of electronic voting for many governments. However, because of the nature of electronic systems, the removal of paper from voting may never be compatible with trustworthy elections.

1.3 The Nedap/Powervote System

The machines to be used in Ireland in June 2004 are classed as DRE (Direct Recording Electronic). That is, votes are cast by inputting preferences to the machine and are recorded directly to storage media within the machine. They are not touch-screen as are the majority of DRE machines used in the USA. Instead, they present the voter with a panel of buttons on which a printed sheet indicates which candidate/option is represented by each button.

Votes are stored on "ballot modules", cigarette packet sized memory cartridges. At close of poll, the contents of the main module are copied onto a backup module which remains in the voting machine unless and until needed. The main ballot modules are collected from the various polling stations and brought to a constituency count centre (in pilots undertaken so far, they were taken by taxi [Fit02]).

At the count centre the modules are read into a desktop PC[1], where the IES (Integrated Election System) count software - written in Borland Delphi and using Microsoft Access - calculates the results. The main vulnerabilities to malicious attack and/or error identified by us so far are outlined in the table below:

Stage:	Vulnerable to:	
	Malice	Error
Development of hardware/software	✓	✓
Storage of machines between polls	✓	
Backup copy		✓
Transport of modules	✓	
Loading of votes from modules	✓	✓
Separation of ballot papers for counting (where multiple ballots are cast on the same day)	✓	✓
Counting results	✓	✓

Figure 1: Vulnerabilties

2 Law

The introduction of e-voting raises questions about the legal position of:

- the electoral rules
- the electoral results
- the vendors of the system

It is vital that the law moves to meet the new challenges posed by introducing new technology.

[1] The number of PCs involved at this stage and the nature of their interconnection is somewhat unclear [see Section 3.2]

2.1 Electoral Rules

The Irish Electoral Act [Ele92] 1992 laid out the rules by which votes should be counted in Irish elections. The act outlined the particular form of Proportional Representation - Single Transferable Vote (PR-STV) mandated in the Irish constitution, including the specific rules to be followed during counting. Thus the Irish Electoral system was completely described in law.

Since the introduction of enabling legislation for electronic voting in 2001, the rules for deciding Irish elections are no longer dictated solely by the relevant law. The software within the system is in fact the final arbiter. Under current agreements between the Irish government and Nedap/Powervote this leads to an extraordinary situation. The count rules no longer belong to the Irish people, are no longer public and are subject to change without legal procedures.

The Electoral Law has been interpreted by the Department in a document called the "Count Rules"[2]. This document serves as the user specification for the programmer. No other documentation exists except the application itself which is in some 150 to 200 modules of Borland Delphi code. The overall codebase is 200,000 lines of code originally established for use in the Netherlands. It has been modified for use in Germany, in Ireland and in the UK. It has recently been further modified for use in a trial in Brest, France. The reviewers' comments [NTec] indicate that there is no separation between the UK and the Irish code base for certain modules. This is a very dangerous practice since the electoral rules are completely different in the two countries - the UK uses "first past the post" whereas Ireland uses PR-STV.

2.2 Electoral Results

In the paper system, the law required that ballot papers be kept for a minimum period of six months in provision for disputes arising. In such cases, a court could require that the paper ballots be re-examined. A similar provision has been made within the electronic system, but as the only records of votes cast would be electronic, the only evidence which could be presented in court would be electronic evidence (or a printout of electronic evidence, which is of course no more reliable). It is difficult to have electronic evidence admitted in a court of law [Lam02] and rightly so, since it is so much more easily manipulated and tampered with.

The legal position of electronic ballots has not been tested in any Irish court, but the possibility that results could be successfully appealed on this basis should certainly be considered.

---

[2] Available for download from http://evoting.cs.may.ie/Documents/DoEHLGCountRules.doc

2.3 Vendors

Electronic voting systems are different from other software and hardware products, because of the vital role they play in the democracies where they are used. It makes sense therefore that the vendors of such products should be treated differently. The commercial interests of those companies cannot be allowed to take precedence over democratic interests.

Perhaps the most obvious conflict between these interests is in the matter of trade secrets. Normal practice within the software industry is for software developers to keep the source code for their products secret. The same applies to all the documentation produced during the development process, including design documents, and test strategies and results.

If the public is to be satisfied that the system was well developed and does what it is supposed to do, this documentation must be made publicly available, so that those with the skills to examine its quality have that opportunity. While this approach prioritises public interests over private, it is not all negative for the company. There are many successful businesses today that use the open source model. For example, the Australian electronic voting system was produced by a commercial company, and its source code is available for download [Aus]. This has already resulted in several flaws being discovered and corrected [Zet03].

A further conflict of interest is this: if there is a flaw in the system it is very much in the public interest that such a flaw be discovered and corrected. This would be bad publicity for the vendor, however. Unfortunately it is not safe to assume that a business will put the correct working of democracy ahead of its own reputation. Therefore it must be made as difficult as possible for vendors to deny or ignore flaws in the system. Again, this requires the highest level of public scrutiny.

The ownership of source code and similar materials (such as design documentation) is another important issue where standard industry practice conflicts with the best interests of the public. Usually software vendors sell licences to use pre-compiled versions of their product and retain copyright of the code itself. However, if the source code were owned by the people instead of the vendors, we would be protected from at least two extremely undesirable scenarios: the case where a vendor or vendors go out of business; and the possibility of vendor refusing to comply with the government's wishes. First, should the vendor go out of business, the future of our electronic voting system would be significantly more secure. There being no doubt as to the ownership of the code, the Government would be considerably freer in their choice of a replacement vendor. Second, since the government would be in a position to switch to a competitor, the vendor could not make unreasonable price increases or other undesirable policy changes, nor could they refuse to make alterations/updates to the software.

The contract between Nedap/Powervote and the Irish Government explicitly retains ownership of the embedded software in the voting machines for Powervote.

> *Clause 10.1.2 Notwithstanding the vesting of ownership of the Ordered Equipment in the Customer, the Customer and Returning Officers acknowledge that the Embedded Software remains subject to a licence granted by the Suppliers and no transfer of ownership of the Embedded Software shall occur, including but without limitation any Intellectual Property Rights in the Embedded Software. The Customer and Returning Officers acknowledge that the Embedded Software is the Confidential Information of the Suppliers.*
>
> http://evoting.cs.may.ie/Documents/DoEHLGPowervoteNedapContract.doc

This is a reversal of the position laid out in the original request for tenders.

> *Clause 8.4 All software paid for and developed to Departments specification will be the property of the Department.*
>
> http://www.electronicvoting.ie/pdf/Req for tenders doc - June2000.doc

The Government has had to provide an indemnity to the Commission on Electronic Voting [CEV] in case the source code it is examining falls into the hands of competitors [Cor04]. To have allowed such a situation to develop shows a significant failure on the part of the Department to set out clear expectations that it should own any software developed for elections. The cost of the software is estimated to be €467,000 for the counting system.

It is vital that these potential conflicts of interest are recognised and addressed by those introducing electronic voting. It is not good enough for a government to rely solely on the advice, opinions and information provided by vendors. These must all be scrutinised by experts with no personal or commercial interest in the system.

3 Politics

The transparency of voting in Ireland, already eroded by the technology of the system itself, is further reduced by the way in which the introduction of the system has been managed. The procurement of evoting is being overseen by a department of the presiding government. The Minister for that department is the director of elections for one of the ruling parties for the upcoming elections. A policy of secrecy is evident, with commercial sensitivity being prioritised over public need to know. This policy is clear from the difficulty faced by those requesting information on the system, as discussed below.

Such secrecy compounds a serious problem inherent in the introduction of technology in publicly sensitive areas. Public understanding of the system is necessarily reduced as the complexity increases. This is unnecessarily exacerbated by a lack of information. Even those with the knowledge to confirm or deny the public's fears and hopes for the system cannot make comment on the suitability of the system.

There is a strong case to be made that the responsibility for decisions regarding voting technology should be taken out of government hands. While this is an issue relevant to politics, it should never become a political issue. An Electoral Commission, such as exists in the UK, would reduce the risk of mixing political motives with public interest.

3.1 Computer Science Meets Politics

Computer science is a relatively new science, only 50 years old, and the public perception of it is quite different from that of other sciences. Perhaps this is influenced by the general availability of computers and their use in practically every aspect of our daily lives. Particle accelerators are not nearly as commonplace as PCs.

No bridge would be built in the developed world without the involvement of an engineer, and yet computer systems are commonly installed by people with minimal knowledge and training. This works adequately in many low-priority situations, and so it may not be obvious that high-priority systems require greater expertise. Similarly, software is generally developed in a very ad hoc manner, which results in high failure rates. Again, this is generally a frustration rather than a major problem and is therefore acceptable in most contexts.

Computer science has, in fact, discovered laws of computation as immutable as those of physics, but the peculiar position of computer science in the public perception makes it very difficult to convey such concepts. While it may sound strange to those with no computer background, computer science tells us that we can never test a computer program enough to be absolutely certain of its behaviour.

NASA, whose employees' lives depend on the reliability of its software, are among the world's most accurate software developers, and yet they provide convincing evidence of this phenomenon. They use sophisticated techniques to reduce the faults in their software to a minimum. But studies have shown that NASA could expect 60 faults to be contained in a software project the size of the Groenendaal counting software[3] [Fis96].

[3] The IES count-software used by the Nedap/Powervote system.

The techniques mentioned above require more resources, including time, than does ad hoc development. So they are generally used only for safety critical applications such as medical equipment and driverless trains. There is a strong argument in favour of the use of these techniques in government applications such as the penalty points system used to keep track of traffic offences in the Republic of Ireland, and in electronic voting. Failures in such systems could result in innocent people going to jail, or the wrong people getting into government.

Because of public perceptions of computer science, people without adequate training may attempt tasks that require deeper knowledge. For instance, the specification of requirements for a computer system is a vital stage that requires certain expertise. It is vital that the specification for a computer system is well thought-out and covers all the requirements for the system. Mistakes made at this stage of system development can have severe effects later in the process.

The resulting lack of consultation with computer professionals has caused many problems in many walks of life, not least in the introduction of electronic voting in Ireland. Failures at the specification stage, which could have been easily identified by computer scientists, remain within the system. The most glaring example of this is the lack of a proper audit trail (see section 1.2).

3.2 Freedom of Information

Given that the people have a constitutional "right to designate the rulers of the state"[4] it is notable that ownership and scrutiny of the casting, collecting and counting of votes has become a secret matter. In response to this, concerned private citizens have made use of the Freedom of Information Acts (1997, 2003 [FoI97]) to obtain as much relevant information as possible.

Attempts to obtain technical details of the electronic voting system in Ireland have been hampered by the exemptions allowed in the Freedom of Information Acts. In particular, The Department of the Environment has relied on the trade secret and the commercial confidentiality exemptions to deny access to most of the documentation from Powervote/Nedap. Surprisingly there is no documentation from Groenendaal on the counting system. In their case the Department has refused to use a section of the Acts which provides that records held by a supplier of services are deemed to be held by the Department. This decision is under appeal to the Information Commissioner.

The Department in 2003 avoided their obligations under this section by virtue of the absence of a formal contract. There was a Letter of Intent in place under which some €30m of equipment and software were purchased. Yet the Department held that there was no current contract.

---

[4] Bunreacht Na h´Eireann/Constitution of Ireland, Article 6.

Other factors inhibiting the public in understanding this system is a marked absence of project documentation, testing schedules and testing results. No end-to-end tests[5] have been independently conducted other than the running of actual pilot elections in three constituencies in 2002. The available reports from this pilot exercise indicate that the normal reconciliation procedures completely failed. The Returning Officer proceeded on the basis of his own judgement that matters seemed to him to be in line with his expectation[6].

Mr. Joe McCarthy's personal requests under the Freedom of Information legislation have cost him €2,882 to date. Every delay allowed under the Act has been used by the Department to frustrate free access to the records. In a letter received on April 23rd, the department again refused to release certain files in the possession of the vendors of the system. Under Freedom of Information legislation, citizens may request records in the possession of "a person who is or was providing a service under a contract for services". The department refused the request on the basis that:

> *This Department does not accept that Nedap Powervote are providing a service for the Department under a contract for services.*
>
> http://www.evoting.cs.may.ie/Documents/DoEHLGDenialofContract.doc

This is in direct conflict with the contract itself (referenced earlier), which in recital 1 establishes a contract for services between Nedap/Powervote and the department.

> *WHEREAS*
> *1. The "Suppliers" will supply to the Department and Returning Officers (as hereinafter defined) designated by the Customer the Equipment (as hereinafter defined), including the Embedded Software {as hereinafter defined), Support, Project and Maintenance Services (as hereinafter defined) and as described in this Agreement.*
>
> http://evoting.cs.may.ie/Documents/DoEHLGPowervoteNedapContract.doc

3.3 History of Electronic Voting in Ireland

The introduction of electronic voting is the biggest change to the Irish electoral system since the establishment of the state over 80 years ago. The idea was introduced by the Fianna Fáil/PD government in 1999 with an Act to allow the use of actual ballot papers for research into voting methods. In 2000 a public tender was issued and it was won by the Powervote/Nedap/Groenendaal consortium.

Later in 2001 an amendment to the Electoral Act was passed allowing the Minister to approve machines for electronic voting. Remarkably, no objective or legal criteria were set for the machines or the software.

---

[5] End-to-end tests are generally considered to be a vital part of the testing process [Tam02].
[6] Paraphrased from comments made during appearances by Mr. John M. Fitzpatrick on Dublin radio station Newstalk106 and national radio station RTE1 on Friday the 16th of April.

The first enabling legislation was brought in as part of a broad, controversial bill. Debate on this bill was guillotined[7] by the Government. Several members voiced their concerns about the system at the time[8]. They were assured that the introduction of electronic voting would not go ahead without all-party consensus.

> *This Government will not proceed without unanimity and general agreement among the Members here.*
>
> - Minister Molloy, Seanad (The Irish Senate), 2001 June 14

The system was then used in three constituencies in the June 2002 General Election. The Government said the trial was successful, but others - including the authors - have grave reservations. The formal reports from the Returning Officers indicate many faults occurred [Fit02]. The results were declared without any external audit of the votes. Without further consultation, either with the Opposition or with the public, the Government decided in October 2002 to implement the system countrywide for the June 2004 local and European elections.

In 2003 a series of reports [Mcg03, Mcc03] were published questioning the integrity of the system and the process used to introduce it. A Parliamentary committee examined the matter but on December 18th 2003 the government parties applied the whip to close the debate just after the authors raised many technical questions. A publicity campaign was launched by the Government in February 2004 costing some €5m.

Public outcry continued to the extent that the Government has now appointed an ad-hoc Commission on Electronic Voting [CEV] to report on the secrecy and accuracy of the system. These terms of reference are narrow and do not allow the Commission to examine the integrity, cost or benefit of the system.

As we write, the Government is intent on pressing ahead in the face of the combined Opposition and with diminishing public support for the initiative.

4 Conclusion

Transparency is an integral part of the security of voting systems. It is vital that technology is not allowed to erode that transparency. Not only must the technology itself implement measures to ensure that it is trustworthy - which, in the current technological climate, means voter verified paper ballots - but the system must be managed in a transparent, non-partisan way.

Where democratic concerns conflict with commercial concerns - as in the case where publication of technical details may threaten intellectual property rights - the democratic concerns must be given priority. After all, businesses can move into other markets. We have only one democracy.

---

[7] This refers to a process whereby a fixed time is set for concluding debate in the Dáil. There is no further discussion at that point, the question is put to the house and voted through by Government majority against the wishes of the Opposition. It is effectively a forced change of the law by the Government.

[8] See Adrian Colley's summary of Dáil and Seanad debates on the subject of electronic voting - http://www.iol.ie/~aecolley/record.html

References

[Aus] Australian electronic voting and counting source code. http://www.elections.act.gov.au/Elecvote.html

[CEV] The webpage of the ad hoc Commission on Electronic Voting: http://www.cev.ie/

[Cha04] David Chaum. Secret-ballot receipts: True voter-verifiable elections. In *IEEE Security & Privacy (Vol. 2, No. 1)*, pages 38–47, January-February 2004.

[Cor04] Mark Brennock Chief Political Correspondent. Last-minute indemnity for e-voting commission agreed. *The Irish Times*, April 2004.

[Ele23] Electoral Act, 1923. Available online at the website of the office of the Attorney General *http://www.irishstatutebook.ie/1923_12.html*.

[Fis96] Charles Fishman. They write the right stuff. *FastCompany*, 06, Dec 1996. http://www.fastcompany.com/online/06/writestuff.html

[Fit02] John M. Fitzpatrick. Dublin county post election report, June 2002. http://evoting.cs.may.ie/Documents/PostElectJune2002.pdf

[FoI97] Freedom of Information Act, 1997. Available online at the website of the office of the Attorney General *http://www.irishstatutebook.ie/1997_13.html*.

[JRB03] Andreu Riera Jorba, Jos Antonio Ortega Ruiz, and Paul Brown. Advanced security to enable trustworthy electronic voting. In *Proceedings of the 3rd European conference on e-Government*, pages 377–384, 2003. http://www.scytl.com/docs/ECEG2003_full_paper.pdf

[Lam02] Paul Lambert. Who has their eye on your online activities? *The Sunday Business Post*, May 2002. http://archives.tcm.ie/businesspost/2002/05/05/story319171.asp

[Mcc03] Joe McCarthy. Report on the IES Counting Software. http://www.evoting.cs.may.ie/Documents/report_oniescountingsoftware.pdf

[Mcg03] Margaret McGaley, J. Paul Gibson. Electronic Voting: A Safety Critical System. http://www.evoting.cs.may.ie/Project/report.pdf

[Mer92] Rebecca T. Mercuri. Physical verifiability of computer systems. In *5th International Computer Virus and Security Conference*, March 1992.

[Mer02] Dr. Rebecca Mercuri. A better ballot box? IEEE Spectrum Online, October 2002.

[NTec] Nathean Technologies. Code review of ies build 0111 for the department of the environment, heritage and local government - page 25. http://www.electronicvoting.ie/pdf/Nathean Code Review Dec03.pdf

[Sch00] Bruce Schneier. Voting and Technology. *Crypto-Gram*, 00(12), Dec 2000. http://www.schneier.com/crypto-gram-0012.html - 1

[Soc04] Irish Computer Society. The ICS calls for audit trail in e-voting system, Mar 2004. http://www.ics.ie/article-027.shtml.

[Tam02] Louise Tamres. *Introducing Software Testing*. Addison-Wesley, 2002.

[U.S] U.S. Public Policy Committee of the Association for Computing Machinery. E-voting technology and standards. WWW page. http://www.acm.org/usacm/Issues/EVoting.htm.

[Zet03] Kim Zetter. Aussies do it right: E-voting. *Wired News*, 2003. http://www.wired.com/news/ebiz/0,1272,61045,00.html

E-Voting in Austria
Legal Requirements and First Steps

Patricia Heindl

Institute of Austrian and European Public Law
Vienna University of Economics and Business Administration
Althanstraße 39-45, 1090 Vienna, AUSTRIA
Patricia.Heindl@wu-wien.ac.at

Abstract: Whereas e-government mainly focuses on strengthening the efficiency of public government processes, it is the goal of e-democracy to improve democratic processes. Law can be defined as a communication-system between the legislative authority and the people. Using electronic media for democratic instruments can make this communication process easier. But there are also dangers and risks.
The topic e-democracy and e-voting is situated at the interface between law, politics and technology. This paper deals with the legal point of view: Which requirements does the law define for internet-based political communication, especially for computer-aided voting procedures in Austria? The law, respectively the constitutional law, defines clear and strict rules for voting and the instruments of direct democracy. If one wants to use computer-aided communication in these fields, the techniques eventually used must fulfil the relevant legal requirements.

1 Introduction

This paper deals with e-democracy and e-voting from the legal point of view. Which requirements does the law, respectively the constitutional law, define for internet-based political communication, especially for computer-aided voting procedures? The paper focusses on the legal analysis of the constitutional and statutory limits and framework. Furthermore, it concentrates on working out the preconditions, de lege lata et ferenda, for e-voting. It will also mention the first statutory amendments of implementing e-voting in Austria.

The topic e-democracy and e-voting is situated at the interface between law, politics and technology: while it is the task of legal research to define the legal preconditions and framework for electronic elections and polls, it is incumbent on technological research to develop electronic voting systems that are able to fulfil the legal guidelines. Technical knowledge is necessary to define the concrete legal issues and demands. The goal of the legal analysis is to work out the legal preconditions for the implementation of such a model.

According to this work it should be feasible to evaluate the risks and opportunities of e-voting. This might aid the Austrian legislator in deciding on the question of whether and in which fields electronic elections and voting could actually be implemented and how the constitutional and statutory principles for this task have to be drafted.

2 Democratic Instruments

Democracy means a form of political decision-making. Article 1 of the Austrian Constitution defines: "Austria is a democratic republic. Its law emanates from the people." Austria has an indirect parliamentary democracy, with some additional instruments of direct democracy. That means that law is not made by the people, but by elected representatives, the parliamentary bodies. Voting is the most important act in political decision-making by the people. Beside that the people can take part in the political decision-making process by three legal instruments of direct democracy: Referendum (Volksabstimmung), popular initiative (Volksbegehren) and public consultation (Volksbefragung).

A referendum is a national plebiscite concerning the enactment of a specific statute. With the – facultative or obligatory – referendum the people can accept or reject parliamentary resolutions at a constitutional level. The positive result of a referendum is binding. At the federal level two referenda have been undertaken so far: one concerning the question of opening a nuclear power station, the other concerning the question of joining the European Union.

The second instrument of direct democracy, the popular initiative, is a formal request by the public to introduce a matter for legislative action in the parliament. With the popular initiative a qualified number of people can raise a law-making initiative. If, at the federal level, more than 100.000 signatures are collected, the "Nationalrat" has to discuss the matter formally. But it will not be obligated to response to the request in substance. So far, there have been over 30 popular initiatives at the federal level. Nearly all of them reached the limit of 100.000 signatures; but almost none of them was followed by the parliament.

The public consultation is the weakest of the three instruments of direct democracy. With the public consultation the parliament merely collects public opinion on a special issue. Contrary to a referendum, a consultation does not have a binding effect but only an advisory character. A public consultation has not yet been undertaken at the federal level, but this instrument predominately is used at the local and regional level.

Election and the named elements of direct democracy are the constitutionally planned instruments in the process of people's decision-making. They constitute the basic democratic instruments. In a wider sense, these also include the pre-forming of political decision-making, particularly performed by political parties, organisations and pressure groups.

3 Democratic Instruments and electronic techniques

Nowadays the internet is not only used for both commercial transactions (e-commerce) and the communication between public authorities and private persons (e-government); it is also gaining ground in the central area of democracy, i.e. election and voting procedures (e-democracy)[1].

Whereas e-government mainly focuses on strengthening the efficiency of government processes, it is the goal of e-democracy to improve democratic processes. Law can be defined as a communication-system between the legislative authority and the people. Using electronic media for democratic instruments can make this communication process easier. But there are also dangers and risks.

Internet-based political communication is conceivable in all the above mentioned fields of democracy. Webpages of political and parliamentary parties or political discussion-forums in the internet are a case in point. But such type of communication is also possible with the institutionalized and constitutionally planned instruments of decision-making. The buzzwords here are "e-voting" and "e-referendum". Clearly the latter case calls for a more stringent legal framework than the former.

4 E-Voting and legal requirements

The law, respectively the constitutional law, defines clear and strict rules for voting and the instruments of direct democracy[2]. If one wants to use computer-aided communication in these fields, the techniques eventually used must fulfil the relevant legal requirements[3].

Elections to parliamentary assemblies (e.g. the federal parliament, regional state parliaments and the European Parliament), the head of state as well as to referenda are governed by constitutional law. In contrary to this elections to institutions representing public or private interests (e.g. unions of any kind) are governed by statutory law.

Considering the instrument of voting, e-voting would have to fulfil the requirements the law defines for traditional voting[4]. Austrian citizens above the age of 18 who are not excluded on account of a criminal conviction enjoy a general, immediate, equal, personal, secret and free right to vote. Austria's electoral system is based on the principle of proportional representation of contending political parties in parliament. That means that the number of votes cast for a party in principle determines the number of its seats in parliament. In general, there are no single-member districts, and no majority system, no principle of "winner takes all".

---

[1] Some authors define e-democracy as a part of e-government; see, e.g., [Sche00].
[2] Art 26, 41 Abs 2, 43, 44 Abs 3, 45, 46, 49b B-VG.
[3] For the following see also [He03], [Ma00], [Po01], [Schr01a], [Schr01b].
[4] Art 26 B-VG and NRWO *BGBl* 1992/471 idF *BGBl* I 2003/90.

Regarding the principle of general voting computer-aided communication does not seem to cause particular problems, given that e-voting is used together with traditional voting. A point yet to be proven is whether it indeed increases voter-turnout and thereby strengthens the principle of general voting. The principle of immediate voting demands that the casted votes have to reach the central voting-teller directly and non-altered. The principle of equal voting demands that each individual can cast her/his vote only once.

Parallel e-voting and traditional voting requires equality between the two voting instruments. For instance, there must be no different information on either of the two voting-"ballots" (eg: programmes of the political parties or information about the candidates). Also different error-filtering procedures might be problematic from the aspect of equality between electronic and traditional voting. Furthermore, e-voting also requires the possibility to cast unvalid votes.

But the greatest problems of e-voting lie in the principles of secret, personal and free voting. E-voting as defined in this paper is casting the votes without the supervision of an official, like voting from one's own computer at home or in the office. From this point of view e-voting poses similar problems as postal voting. In both cases the votes are not given within a secure polling booth, but the voters themselves must look for the secret and free voting act. Therefore postal voting in political elections is allowed only in some states – predominately in exceptional cases. In those states that allow postal voting – like e. g. Switzerland[5] in general or Germany[6] in exceptional cases – the constitutional barriers for e-voting seem lower than in states which have no right of distant voting.

The Austrian Constitutional Court decided, that postal voting is unconstitutional because it infringes the principles of personal and secret voting[7]. A few years later another decision by the Austrian Constitutional Court held, that Austrian nationals living abroad, must not be excluded from the right to vote only due to the lack of a permanent residence in Austria[8]. Following that a constitutional amendment was undertaken: Austrians abroad, e.g. Austrian citizens resident abroad or just staying abroad, may also vote in embassies and consulates. Even a vote in the presence of a witness will suffice. The latter case can be turned "quasi-postal" voting for Austrians abroad.

The special challenges of e-voting are twofold. On the one hand the techniques must satisfy that only legally entitled people can cast their votes and this only once. Also technical protection against electronic election fraud by hackers or technical breakdowns is necessary. On the other hand the techniques must guarantee that identification of the voter is impossible. In other words: both must be guaranteed: identity of the elector and authenticity of the casted vote and at the same time strict anonymity of the ballot paper.

---

[5] See, e.g., *Braun* in this book.
[6] See, e.g., *Volkamer* in this book.
[7] VfSlg 10.412/1985.
[8] VfSlg 12.023/1989.

Furthermore, e-voting, like traditional voting, must also allow for the possibility of ex-post examination of the election result: therefore the election-data have to stay accessible after the election day in an adequate way.

Another point is the future role of the constitutionally planned government officials in an e-voting and e-counting process.

Arguments outlined for e-voting also apply to e-referenda and e-public-consultation. E-referenda and e-voting are thus the most challenging and delicate fields of e-democracy.

The legal requirements for an "e-popular initiative" seem comparatively easier to fulfil. Here only authenticity, but no anonymity is required. From the political point of view computer-aided political communication in this element of direct democracy might have the most practical relevance. Because of electronically collecting the large numbers of signatures involved is much less time consuming and less costly than the traditional type of signature collection. This might not only lead to more frequent use of this instrument. It might also inhence opportunities to raise political initiatives for smaller and less institutionally organized groups.

5 Implementation

The implementation of e-voting for political elections of the first level (i.e. elections to the head of state, the federal parliament, regional state parliaments and the European Parliament as well as to referenda) is unconstitutional and would require a constitutional amendment. By contrast for implementing e-voting for elections to institutions representing public or private interests (e.g. unions of any kind) statutory amendments are sufficient. This is because here the voting principles are statuted not on a constitutional but on a statutory level and there is no principle of personal voting[9].

In the latter case the Austrian legislator has already taken the first steps: legal provisions for e-voting already exist for the Austrian Union of Students as well as for the Austrian Chamber of Economics[10]. Still the concreting statutory orders are missing.

Until now there have been no legally binding electronic elections in Austria. However, a first test of e-voting was undertaken parallel to the elections of the Austrian Federation of Students at the Vienna University of Economics and Business Administration[11]; another test was undertaken recently parallel to the elections of the Austrian Head of State. The implementation of e-voting in elections for unions and chambers like the named or other institutions, might help to stop the steadily declining number of people casting their votes.

---

[9] *VfSlg* 8.590/1979, 14.440/1996.
[10] § 34 Abs 4 ff *HSG*, *BGBl* I 2001/18; § 74 Abs 2 ff *WKG*, *BGBl* I 2001/153.
[11] See [Kr03], [Me01], [SK00].

Provided that all technical problems with e-voting can be solved and the legal provisions mentioned above can be fulfilled, there would still remain issues to be settled. Above all the fact of distance-voting and – in a more sociological sense – the necessarity of trusting the electronic techniques by the electors. As mentioned above: absolute protection of the secrecy voting act can not be guaranteed. If the Austrian legislator would in the future decide to implement e-voting in political elections, this possibility should always be restricted to those groups who are not able to cast their votes within the official polling booth.

References

[He03] Heindl, P., e-voting und e-democracy aus verfassungsrechtlicher Sicht, in: E. Schweighofer et al (Hrsg.), Zwischen Rechtstheorie und e-Government, Wien 2003, 279 ff.

[Kr03] Krimmer, R., E-Voting in Österreich, in: E. Schweighofer et al (Hrsg.), Zwischen Rechtstheorie und e-Government, Wien 2003, 271 ff.

[Ma00] Marschitz, W., Internetvoting, in: Österreichische Monatshefte (2000), http://www.plattform.or.at/download/POP_Art_Internetvoting.pdf (15. 1. 2004).

[Me01] Menzel, T., E-Voting an österreichische Hochschulen, in: E. Schweighofer et al (Hrsg.), Auf dem Weg zur ePerson, Wien 2001, 281 ff.

[Po01] Poier, K., Grundrechte und E-Voting, in: Österreichische Juristenkommission (Hrsg.), Grundrechte in der Informationsgesellschaft, Wien 2001, 102 ff.

[Sche00] Schefbeck, G., Elektronische Demokratie, in: E. Schweighofer, T. Menzel (Hrsg.), E-Commerce und E-Government, Wien 2000, 89 ff.

[Sche01] Schefbeck, G., Aktuelle Trends in der E-Demokratie, in: E.Schweighofer et al (Hrsg.), Aufdem Weg zur ePerson, Wien 2001, 293 ff.

[SK00] Schinagl, W., Kilches R., Online Wahlen und E-Voting – Entwicklungstendenzen zu elektronischen Wirtschaftskammer-Wahlen im Jahr 2005, in: D. Pauger (GesRd.), Neue Medien – 3. Fakultätstag der Rechtswissenschaftlichen Fakultät 12. Mai 2000 (oJ.), 291 ff.

[Schr01a] Schreiner, H., Art 26 B-VG, in: H. P. Rill und H. Schäffer (Hrsg.), Bundesverfassungsrecht – Kommentar, Wien 2001, Rz 57.

[Schr01b] Schreiner, H., Wahlen per Mausklick – rechtliche Überlegungen zum I-Voting, in: E.Schweighofer et al (Hrsg.), Auf dem Weg zur ePerson, Wien 2001, 258 ff.

Security Assets in E-Voting

Alexander Prosser, Robert Kofler, Robert Krimmer, Martin Karl Unger

Institute for Information Processing, Information Business and Process Management
Department Production Management
Vienna University of Economics and Business Administration
A-1200 Vienna, AUSTRIA
[Alexander.Prosser | Robert.Kofler | Robert.Krimmer | Martin.Unger}@wu-wien.ac.at

Abstract: As discussed in the literature [PrMü01; Rub04; Phi02] e-voting faces a lot of threats. The purpose of this paper is to give a systematically ordered overview of attacks against e-voting and to show one solution to the issues. The challenge is to provide identification and anonymity at the same time and to exclude the possibility of fraudulent manipulations by the server administration, the voter, and any third party.

1 Protocol Issues

1.1 Two-Stage Versus One-Stage Voting Protocols

In a fundamental contribution, Nurmi et al. [NSS91] identified two building blocks in an electronic voting system: (i) Voter identification and registration for e-voting and (ii) vote casting. These steps can be provided in one Internet session (one-step protocol); but here the identification may be used to trace the identity of the vote via the IP address or temporary files. This issue is avoided by a two-stage procedure, which strictly separates voter identification and vote-casting. But the advantage comes at a price, as the result of successful identification (voting token) has to be stored at the voter to be used later to cast a vote. Figures 1a and 1b provide an overview of the two stages.

Registration phase:

The voter applies for a voting token. The system performs a check of his credentials and a check for multiple application. If this is his first attempt, the voter will receive a voting token which he can use anonymously to cast a vote later. If not, the system performs a restart procedure, which always issues the same token to the applicant, which is stored in the database of the regis-tration service.

At the end of the process, the voter checks the authenticity and integrity of the token and stores it either on a smart card or on another media, e.g. a USB token.

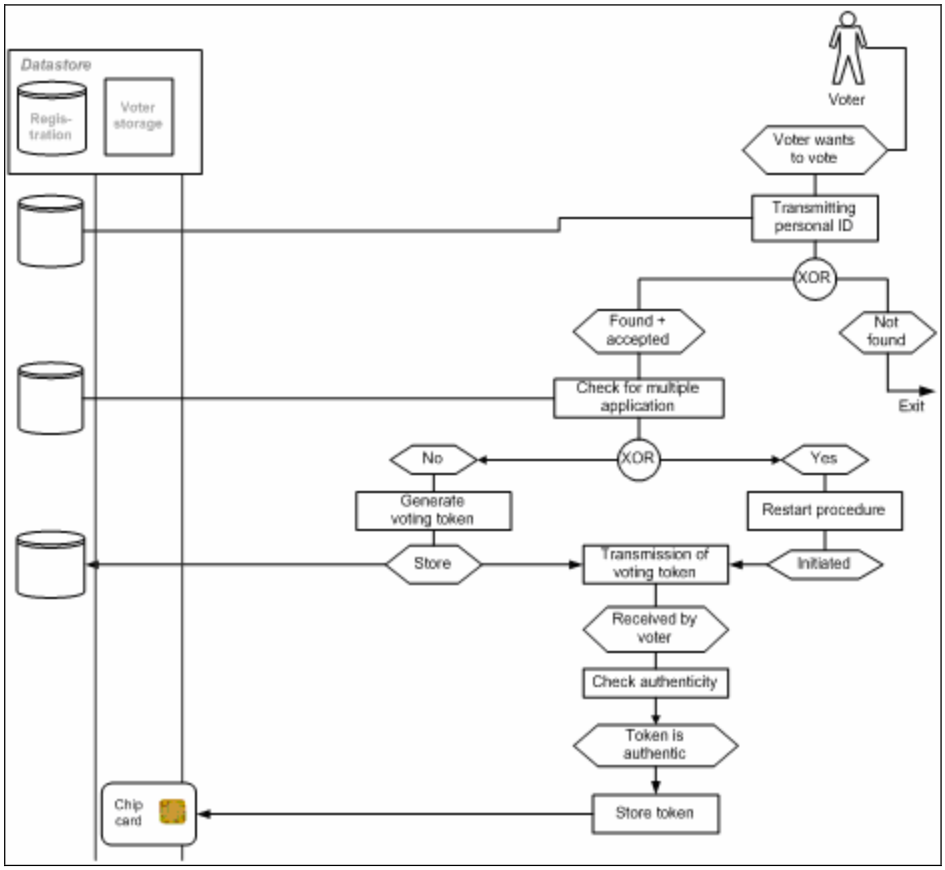


Figure 1a: Registration phase

Voting phase:

The voting application reads the voting token from the storage device and sends it to the ballot box system, which verifies its authenticity and checks for duplicates. If the checks are successful, the voter will receive a ballot sheet, which must be protected against manipulation. The voter fills in the ballot sheet and casts a vote. There is a precaution mechanism that challenges the voter before the vote is actually cast to prevent precipitate or "junk" votes.

Finally the voter receives a confirmation that the vote has been cast successfully.

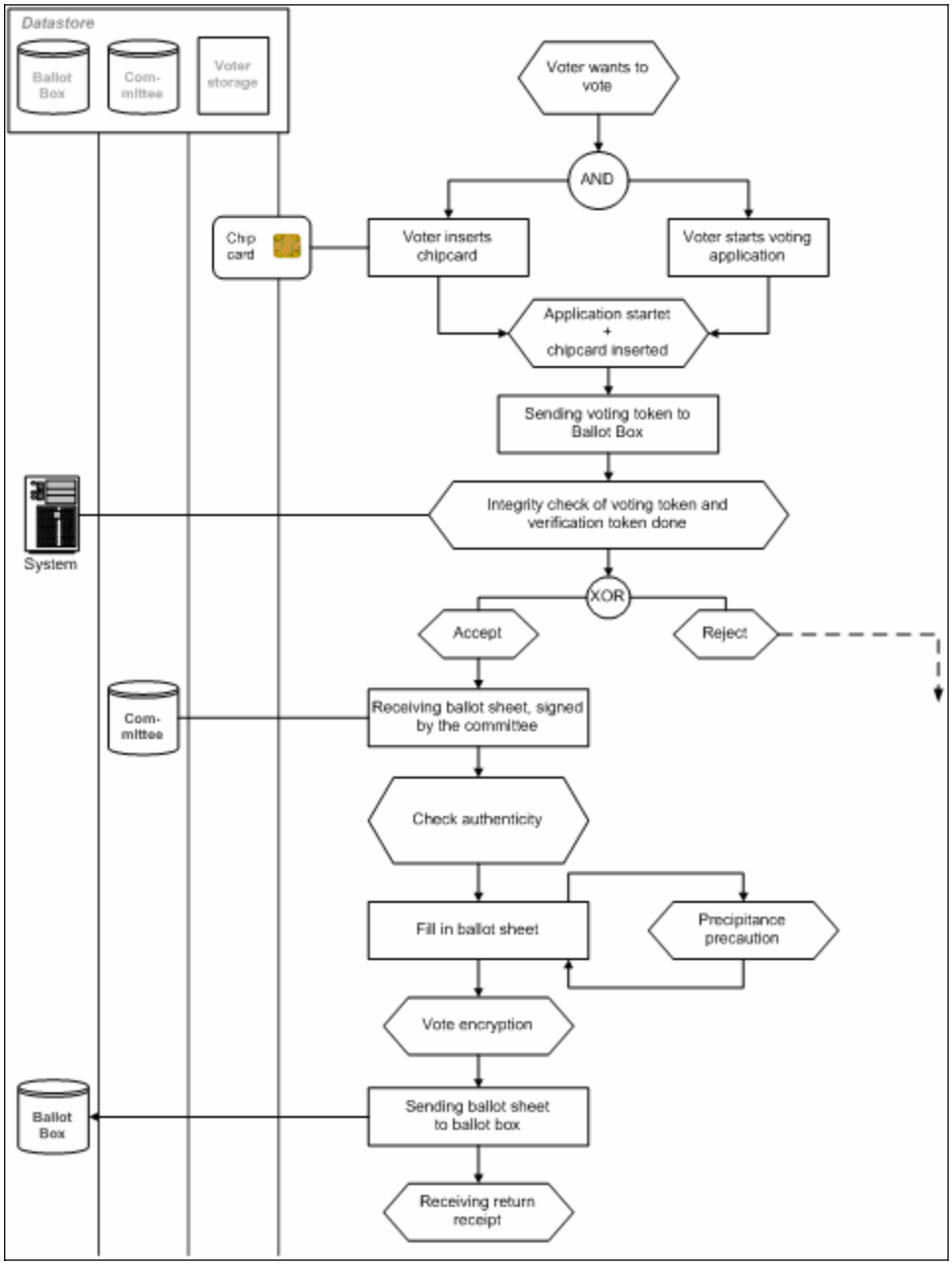


Figure 1b: Voting phase

Eventually, there may also be also a facility for the voter to check whether his vote was counted correctly and entered the tally.

1.2 Threat Scenarios

1.2.1 Threats during Registration

Beginning with the initiation of the process there must be a possibility to verify the authenticity of the voter's application and/or visited webpage [FFW99]. The next step is the application for the selected election (there can be more than one election at the same time). When the user transmits his personal ID or related information, it must be protected from modification, re-send attacks, content sniffing (the fact whether somebody is going to vote should remain private) and all forms of faked identities. The voter's identification and assignment to a constituency must be established beyond doubt and must be protected from manipulation by the voter as well as by the system administration.

Also the constituency the voter belongs to should be protected from manipulation (eg., a voter "re-registers" himself to another constituency, where he perceives that the vote would probably have a higher marginal value). This is particularly an issue in two-stage voting protocols, as the token issued on registration must be used anonymously and hence, has to include the constituency information, so that the vote can be assigned correctly, even though the voter will not be identified at the voting stage.

On the voting server side, it must be assured that multiple (malicious) applications from one person can be handled. The Server administrator must not be able to change a voter's constituency without detection; also selective denial of service to registrants by the administration must be prevented. In addition, the administration must not be able to create fake voting tokens or to-kens on behalf of people, who did not register.

Furthermore the administrator must not delete records from the registration database unrecognized. An audit trail must be producible that links every voting token issued to an eligible voter, showing that every voter also had the opportunity to obtain a voting token but once.

When the voting token is received by the client, some integrity checks should be done before the token is stored on a secure media or if no secure media is available we need equivalent methods to prevent others from using it (eg, a third person, Trojan, virus or other malign application).

1.2.2 Threats during the Voting Phase

Authenticity, validity and integrity of a voting token must be assured, at the same time, the token must be usably in a completely anonymous way. The voter uses the token to apply for a ballot sheet. It has to be assured that the ballot sheet is not modified during transmission by a man in the middle or by the administrator of the ballot box - therefore the voter needs some guarantee that this is the correct ballot sheet he applied for. Duplicate use of voting tokens has to be prevented.

Also, it has to be assured that ballot sheets cannot be manipulated by the server administration and are delivered to the voter authentically. When the voting software renders and displays the ballot sheet, it should use a secure viewer so that no virus or Trojan horse application can neither change the ballot sheet, nor forward the voter's choice to a third party. As the content of the vote should be kept secret even from the election system administration until the ballot box is opened, the vote should also be encrypted in a way that the administration cannot read or manipulate the vote.

The ballot box server environment must prevent the administration from denying access, deleting, inserting or modifying ballot sheets and it must prevent multiple usages of voting tokens. In a two-stage protocol the administrator must not be able to separate the voting token from the ballot sheet. And most importantly, voter anonymity must be guaranteed vis-à-vis the election administration as well as any third party.

The last step in the voting process is a return receipt which shows the voter that his ballot sheet was received. However, no proof must be possible, how a voter voted, as this would enable vote buying and pressured votes. On request, an audit trail must be produced linking the token used and the fact that a ballot sheet was obtained and stored. This audit trail must not corrupt anonymity, but it has to be manipulation-proof, also by the election administration. This also serves as a defence against unfounded objections and complaints from voters, candidates or third parties maintaining irregularities in the voting process in order to sabotage or discredit the election.

1.2.3 Levels of Security

In the discussion of e-voting security, one has to distinguish between organizational and technical security. Precautions are organizational, if they rely on the behaviour of agents and their compliance to rules. Examples would be

- Information stored on two server systems, which, once joined, would corrupt anonymity; the server administrators are obliged (possibly under oath) not to communicate data.
- Servers locked into a safe room to prevent tampering.
- A witness, who (digitally or on paper) signs that a certain document was filled in at a certain time and in a certain place.

Technical precautions provide a technical guarantee against defined manipulations or threats; it does not rely on any agent's compliance with proper procedures. Examples would be

- Cryptographic encoding of ballot sheets to prevent their manipulation by the server administration.
- A blind signature [Chau82] or ANDOS [BCR87] procedure to prevent the tracing of voting tokens.

It should be noted that technical security cannot be absolute – at some stage organizational security has to come in. Digital signature cards, for example, provide an extremely high level of technical security; however, when the card is issued,

organizational precautions against manipulations are necessary to prevent, for example, the card PIN entered by the card holder from being recorded and later to be used in conjunction with the stolen signature card. Hence, the decisive question is, at which level technical security ends and where reliance on organizational measures starts. The following section provides a model to asses this issue in the field of e-voting.

2 Six Aspects of E-Voting Security

Six aspects can be identified in e-voting security to be fulfilled either by organizational or technical/algorithmic arrangements. The degree to which an e-voting system relies on technical security constitutes the essential quality parameter of such a system [IPI01].

The aspects are: (i) Permanent voter anonymity, (ii) voter identification and ascertainment of eligibility, (iii) resistance against all forms of manipulation (third party, voter or administration staff), (iv) prevention of vote buying, (v) a complete audit trail for authorities and voters, (vi) prevention of sabotage and attempts to discredit the election. Figure 2 summarizes these dimensions defining a 4 point scale for each dimension (from within: (1) slight to no protection, (2) corruptible with medium determination, (3) high degree of protection, (4) virtually unbreakable). For each dimension, the model defines how far technical safeguards apply (the line joining the dimensions). Beyond this level, organizational safeguards may apply. However, it remains to be ascertained from case to case, whether organizational protection is viable.

Some of the above goals are in clear antinomy. An e-voting system, for example, designed to perfectly meet requirements (ii) to (vi) cannot technically guarantee voter anonymity (see Figure 2). In this case, organizational safeguards would have to be provided.

On the other hand a system, designed to meet the requirement of anonymity only (“naive anonymity”) would neglect the other goals and would have to provide purely organizational safe-guards (Figure 3).

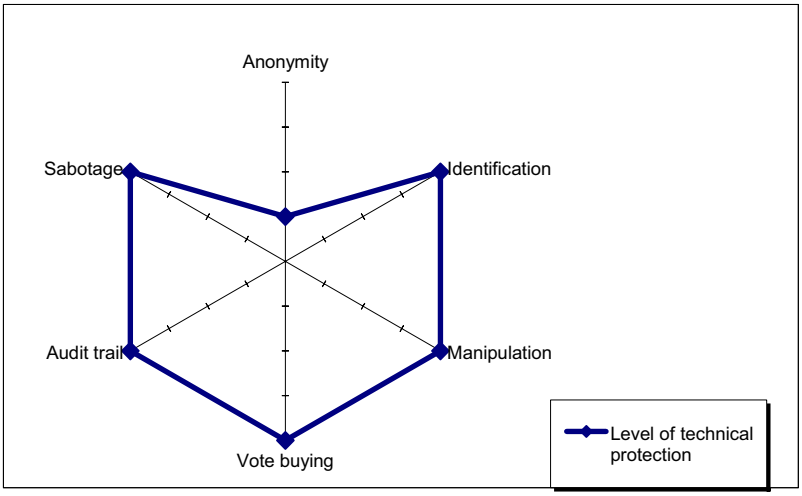


Figure 2: Fully auditable system, resistant against sabotage and manipulation

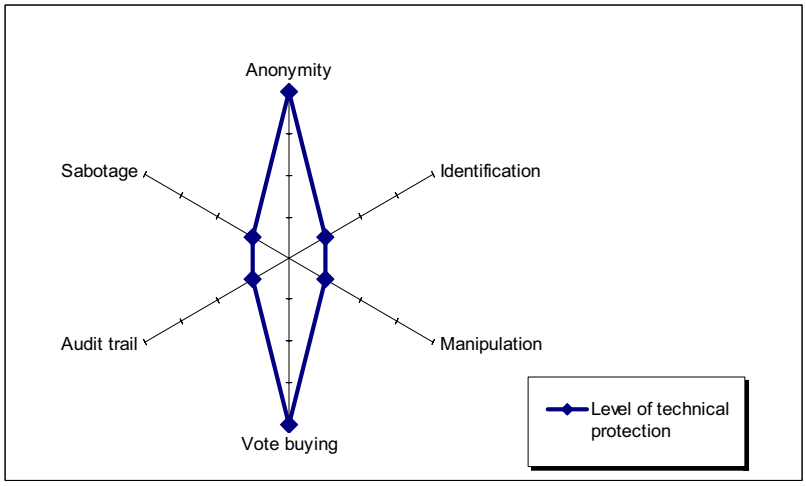


Figure 3: "Naively" anonymous system

The question arises, whether a voting protocol can be defined that combines technical safe-guards for voter anonymity as well as identification and reproducibility.

3 The Protocol of e-voting.at

The participating parties are (i) the voter, (ii) the registration authority maintaining the voter register, (iii) the electronic ballot box, (iv) a third party, such as a trust centre or the Privacy Protection Committee.

Registration:

1. The registrator has one signature key pair (e, d) per constituency c; each trust centre participating in the election has its (ε, δ).
2. The voter sends his voter ID to the registrator, which after checking the voter's eligibility answers with *c* and the appropriate e. The voter also polls the trust centre for ε.
3. The voter creates random tokens t and τ preparing them for a blind RSA signature ($b(t), b(\tau)$). c, $b(t)$ and a standard text applying for a signed e-voting token is sent to the registrator, which after checking the credentials again blindly signs and returns $d(b(t))$. The voter removes the blinding layer and obtains $d(t)$.
4. The voter obtains $\delta(\tau)$ in a similar way from the trust centre.

Storage:

The voter stores $t, d(t), \tau, \delta(\tau), c$ on a secure media (for the role of smart cards in e-voting, cf. [PKKU04]).

Voting:

1. Prior to the election, the members of the election committee form RSA key pairs (k, k') and make their respective encryption keys k' known to the ballot box server.
2. On election day, the voter sends $t, d(t), \tau, \delta(\tau), c$ to the ballot box server, which knows all relevant e and ε.
3. If the ballot box can authenticate the tokens for the constituency indicated and if they have not already been used, it returns an empty ballot sheet BS and the relevant k'.
4. The voter codes the filled-in BS with k' and untamperably links the tokens to this $k'(BS)$. The ballot box once again checks the tokens and stores the ballot.
5. The ballot box issues a receipt, which does not contain any information on the vote cast.

After the election finished, the members of the election committee reveal their secret decryption key k and the ballot sheets are decrypted. The above protocol as currently implemented does not enable majority decisions by the election committee, or enables the replacement of an election committee member who had an accident, lost his key, wants to sabotage the election etc. A solution for quorum-based decisions is provided in [PKKU04a].

4 Threats and Security

Let us analyze the security aspects identified in Figures 2 and 3:

Anonymity
Since the token is issued with a blind signature it cannot be traced back to the user. On election day, the voter uses the token as means of authentication only. The only means of intercepting the token and to corrupt anonymity is the voter's PC. This can be ruled out, if the decisive parts of the voting protocol (such as the resolution of the blind signature provided by the registration server) are performed in the secure environment of a smart card (eg., a signature card).

Identification
Authenticity can be provided by signing the application for a voting token using a digital signature card. If this is also a citizen card (in Austria cf. [HoKa04]), the voter can also be identified. Authenticity on election day is only provided by the voting token. If this token is not stored in the secure environment of a PIN protected area on a smart card, the token has to be password-protected.

Manipulation
Manipulation by a third party can happen in transmission or on the voter's PC. The former is prevented by standard encryption, such as SSL/TLS (IETF RFC 2246), the latter by again performing the decisive protocol elements in a secure and tamper-proof environment.

Manipulation by the administration can affect:
(i) The issue of fake tokens, which is prevented by the second authority, whose token is needed to cast a vote as well.

(ii) The manipulation of votes, which is prevented by encryption of the ballot sheet with the keys of the members of the election committee.

(iii) The insertion of votes, which is prevented by the same mechanism as (i) and by the fact that the token is re-submitted and inextricably linked to the filled-in ballot sheet when it is submitted.

(iv) The deletion of votes can be prevented when the tokens are published for which a vote was cast and voters are provided with a signed conformation by the ballot box server that a vote has been cast for this token.

Vote Buying
The voter is given a receipt without any reference to the actual vote cast. This would also be impossible, as the vote submitted to the ballot box server is coded with the election committee keys.

Audit Trail
The audit trail is two-fold corresponding to the two-stage protocol: (i) it is reproducible, which member of the electorate sent in a signed application to vote electronically and

whether she received a token; (ii) which token was sent in to obtain a ballot sheet and which vote was cast for the respective token. Of course, the link between (i) and (ii) is not reproducible; this is the essence of a two-stage protocol. (iii) Each signed application must contain a corresponding one from a second authority.

Sabotage

Since there is a complete audit trail, assertions of irregularities can be dealt with satisfactorily.

The protocol described in this paper has been implemented and used in two test elections parallel to the Student Union election in 2003 [PKK03] and the Austrian Federal Presidential election in 2004 [PKKU04b].

References

[BCR87] Brassard, G., Crepeau, C., Robert, J.-M.: All-or-Nothing Disclosure of Secrets. In: Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86, Berlin, Springer-Verlag, 1987, pp. 234-238

[Chau82] Chaum, D.: Blind Signatures for Untraceable Payments in: Chaum, D., Rivest, R.L., Sherman A.T. (eds): Advances in Cryptology, Proceedings of Crypto 82, pp. 199-203

[HoKa04] Hollosi, A., Karlinger, G.: Einführung in die österreichische Bürgerkarte; Bundeskanzleramt, Stabsstelle IKT-Strategie des Bundes, Technik und Standards, Vienna, 2004, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html (10.6.2004)

[IPI01] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC), 2001 http://www.internetpolicy.org/research/e_voting_report.pdf (2001-11-20)

[FFW99] Feghhi, J., Feghhi, J., Williams, P.: Digital Certificates – Applied Internet Security; Addison-Wesley, Reading, 1999

[NSS91] Nurmi, H., Salomaa, A., Santean, L.: Secret ballot elections in computer networks; Computers and Security 36 (10), 1991, pp. 553-560

[Phi02] Philippsen M.: Internetwahlen – Demokratische Wahlen über das Internet; Informatik Spektrum 25(2) 2002, pp. 138-150

[PKK03] Prosser, A., Kofler, R., Krimmer, R.: Deploying Electronic Democracy for Public Corporations. In: Traunmüller, R. (ed.): Electronic Government, LNCS 2739(2003), pp. 234-239

[PKKU04] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: The Role of Digital Signature Cards in Electronic Voting. Proceedings of 37th Annual Hawaii International Conference on System Sciences (CD/ROM), Computer Society Press, 2004

[PKKU04a] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: Implementation of Quorum-based Decisions in an Election Committee; to appear in Traunmüller, R. (ed.) E-Government; Lecture Notes in Computer Science, Springer, 2004

[PKKU04b] Prosser, A., Kofler, R., Krimmer, R., Unger, M.K.: e-Voting Wahltest zur Bundespräsidentschaftswahl 2004, Arbeitsbericht zum Tätigkeitsfeld Wirtschaftsinformatik, Informationsverarbeitung und Informationswirtschaft 01/2004, Wirtschaftsuniversität Wien, 2004

[PrMü01] Prosser, A., Müller-Török, R.: Electronic Voting via the Internet; Int. Conf. on Enterprise Information Systems ICEIS 2001, Setùbal, pp. 1061-1066

[Rub04] Rubin, A.: Security Considerations for Remote Electronic Voting over the Internet http://avirubin.com/e-voting.security.pdf (23.5.2004)

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Language to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER - Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods - Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahnič (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3.Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 - Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement - Erfahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometric and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society

The titles can be purchased at:
Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14
53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de