BITS OR PAPER? COMPARING REMOTE ELECTRONIC VOTING TO POSTAL VOTING

Robert Krimmer[1], Melanie Volkamer[2]

In the recent years it has often been discussed how elections can be conducted via the Internet. Many countries, including Germany, Estonia, Great Britain, Switzerland, USA or Austria have run tests of implementing e-Voting on different levels. Whilst offering e-Voting for public elections implies various legal problems, associations can allow for e-Voting in a relatively easy way. In this paper we investigate an election run by the leading German non governmental organization (NGO) in information technology – the Gesellschaft für Informatik (GI) – that provided for remote voting using postal voting and electronic voting via the Internet. It is a common requirement by election officials for remote e-Voting to be as secure as regular postal voting. To come up with an assessment the use of a criteria catalogue is best to compare these forms of voting.

1 Introduction

With the rising use of the Internet and the transformation of paper based transaction processes into electronic enabled online applications it was only a matter of time till the first projects thought of an electronic voting process. So in the recent years many organisations have thought about such an application out of different reasons[3]. One of the reasons has often been to raise the participation rate of the electorate. In many cases the way to do so was introducing remote voting either on paper (postal voting) or electronically (remote e-Voting). Both methods share common problems like family voting but also have contradictory problems like securing the anonymity.

As elections in general are processes developed over time and closely tied to a country's or organisation's history, e-Voting projects vary a lot. As the development of applications for support of the democratic processes is very demanding and costly, international best practices and experiences are searched for intensively. Still due to the nature of democracy applications they are very individual and therefore it is difficult to compare them without taking certain pre-conditions into account.

Whilst in the field of e-government yearly benchmarks are organized by Cap Gemini [2], first comparative studies in the field of e-democracy (i.e. including e-participation and e-Voting research) have been conducted by Macintosh [3], Braun et.al. [4], and Kersting [5]. The most comprehensive study on e-Voting in Europe has been organized by Leenes and Svenson [6].

All studies found that the context of the e-democracy applications influenced the way of implementation massively.

[1]University of Linz, Institute for Informatics in Business and Government, Altenbergerstrasse 69, A-4040 Linz, e-mail: krimmer@iwv.jku.at

[2]German Research Center for Artificial Intelligence DFKI Saarbrücken, Stuhlsatzenhausweg 3, D-66123 Saarbrücken, e-mail: volkamer@dfki.de

[3]For an overview of European e-Voting projects see the proceedings of the ESF TED workshop on Electronic Voting in Europe in [1]

In an effort to develop a criteria catalogue for comparison of e-Voting projects the approach in [7] is to differentiate between different preconditions that usually influence the way elections are held. They differentiate them in four dimensions, i.e. (1) technology, (2) law, (3) politics and (4) society.

Further more during the introduction of e-Voting legal regulations require remote e-Voting to provide for the same level of security as any other form of remote voting, i.e. postal voting. In order to assess these services for their level of security it is necessary to compare the specific conditions and processes of the remote voting channels based on a criteria catalogue. So we modified the previous mentioned catalogue to fit our purposes of comparing two remote voting channels in a practical experience. Further we chose the election of the Gesellschaft für Informatik (GI)[4]. It is a perfect place to undertake such an investigation as it is a community of technology-fit users but share a critical point of view towards innovations in the information science field.

In this article we first come up with common problems of remote elections and then introduce the criteria catalogue. We continue with the case study of the GI election using the catalogue and finally give an assessment towards the issues of remote elections.

2 Shared Problems and Risks of Remote Voting

As it is shown in [8] postal voting and remote electronic Voting are distance election forms and so there are some common problems concerning the free and secret election principle. This is because casting the vote does not take place in a secure environment like in a polling booth positioned in a polling station but in a private environment. Therefore a local election committee cannot ensure that a voter can cast her vote in secrecy. Similar problems arise in respect to the free election principle due to problems like family voting, electoral enforcement and vote buying. So now it is not the election committee but the voter who has to protect the election principals of a free and secret election.

In [8], the authors compare the new remote electronic voting to the already existing postal voting in regard to a security point of view. With the usage of postal voting, there exist difficulties in respect to the secret, equal and universal election principals. The problem to ensure a secret election arises from the fact that the voting material is sent to the election administration in one envelope. So an attacker could catch the labelled letters on their way from the voter to the election administration and open them. Further problems arise from the mail delivery time whereby the equal and universal election principles may be at risk, but those are common postal delivery problems.

Using a remote e-Voting system, the main problems concern the secret, free and universal election principals and are due to the insecurity of the voter's PC. We can think of several attacks involving Trojan horses: One would be that the Trojan horse would send the cast ballot unencrypted from the voter's PC to the attacker (violation against the secret election principal) or the Trojan horse could change the ballot on the voter's PC before it is sent it to the election server (violation against the free election principal). All of this could be done without any further input or notice of the computer user and done completely automatically. And at last the universal election is endangered because of denial of service attacks.

[4]The Gesellschaft für Informatik (GI) was set up in 1969 in Bonn as a registered association. Its intention is to promote the computer science. The GI's electoral laws are bound in the articles of association (see [9]-[11]) and the election reulations (see [12]). For the rest of this paper we will use the short cut.

3 Criteria Catalogue

The comparison of e-Voting projects is very difficult as they normally represent very individual developments for the respective organisations or nations as it was shown in the cross-national studies [3]-[6]. This criteria catalogue is a modified version of the second part from the one available in [7], especially refined to compare a traditional paper based remote voting channel to a remote e-Voting channel. It consists of three parts: (1) a *project overview*, (2) the *technology* used, and (3) the *outcome of the project*. So our main focus it the technology because law, politics and society are the same for both types of elections.

In the following we will use this criteria catalogue to assess the use of postal and remote electronic voting in the GI election 2004.

1	**Project Overview**	2.2	Procedural Issues
1.1	General Project Description	*2.2.1*	*Postal Voting Procedure*
1.1.1	*Form of Voting Used*	*2.2.1.1*	*Election Principles (Free, Equal)*
1.1.2	*Status*	*2.2.1.2*	*Kind of Identification*
1.1.3	*Duration*	*2.2.1.3*	*How to Guarantee Anonymity*
1.1.4	*Sustainability*	*2.2.1.4*	*Double Voting Protection*
1.1.5	*Location of Tests (Public/Private)*	*2.2.1.5*	*Protection against Ineligible Voters*
1.1.6	*Aim*	*2.2.1.6*	*Protection against Counting of Votes before End of Election*
1.2	Resources	*2.2.1.7*	*Identification of Fraud*
1.2.1	*Budget (amount, funds)*	*2.2.1.8*	*Possibility of Checks and Balances by Election Committee*
1.2.2	*Actors*	*2.2.2*	*Remote eVoting*
1.2.2.1	*Whose initiative*	*2.2.2.1*	*Election Principles (Free, Equal)*
1.2.2.2	*Level of Governmental/Organizational Support*	*2.2.2.2*	*Kind of Identification*
1.2.2.3	*Positions of Actors*	*2.2.2.3*	*How to Guarantee Anonymity*
1.2.3.4	*Scientific Background*	*2.2.2.4*	*Double Voting Protection*
1.3	Scope	*2.2.2.5*	*Protection against Ineligible Voters*
1.3.1	*Legal Validity*	*2.2.2.6*	*Protection against Counting of Votes before End of Election*
1.3.2	*Participants and Turnout*	*2.2.2.7*	*Identification of Fraud*
1.4	Promotion	*2.2.2.8*	*Possibility of Checks and Balances by Election Committee*
2	**Technology**	2.3	Security of Remote eVoting
2.1	General	*2.3.1*	*Examination and Certification of System*
2.1.1	*Postal Voting*	*2.3.2*	*System Stability and Load Balancing*
2.1.1.1	*Process of Postal Voting*	*2.3.3*	*Organisational Surveillance of System*
2.1.1.2	*Failure Rates of Mail Delivery*	*2.3.4*	*Crisis Management Guidelines*
2.1.1.3	*Quality of Mail Addresses*	*2.3.5*	*Defense against DOS Attacks*
2.1.2	*Remote eVoting*	*2.3.6*	*Defense against Viruses, Trojan Horses*
2.1.2.1	*Hard- and Software Used*	*2.3.7*	*Protection against Spoofing, Man-in-the-middle-Attack, Security*
2.1.2.2	*Developer and/or Provider*	*2.3.8*	*Organizational Measures against Access to the Servers*
2.1.2.3	*Forms of eVoting Used*	2.4	Rules of Engagement
		3	**Outcomes**
		3.1	Results of Evaluation
		3.2	Other Outcomes
		3.3	Critical Success Factors
		3.4	Contentedness of the Voters

Table 1: Criteria catalogue to compare e-Voting with postal voting within a concrete example

4 The Case Study

In Germany in the current past, three associations applied an e-Voting system for legal binding elections[5]. The most popular one and the one with the largest amount of voters, in December 2004, was the GI's chairman election. They used the remote e-Voting and postal voting and so it is a very good example for our case study. In the following we will apply the criteria catalogue to compare the security of postal voting with the one of remote e-Voting[6].

[5]The associations are the GI, the D21 [13] and the Digitale Brücke [14].

[6]We used only material provided to the public either by web research or by reference from the GI or Micromata, which can be found in the references [15] – [22].

4.1 General Project Overview

4.1.1 General Description

The voters had the possibility either to use remote e-Voting form their own PCs or they could use postal voting (*type of project*). The election was a pilot project[7], but never the less it was legal binding (see election information letter) (*status of the project*). Since the GI articles for voting have been changed it is possible to use e-Voting for all GI elections. The main process to offer e-Voting as an additional voting channel in an election started in 2003. The management board presented their request to the chairmen in January of 2004 and the chairmen agreed. In autumn 2004 the chairmanship decided to use Micromata's POLYAS system for the next chairman election. Finally the POLYAS system was in operation from the 15th of October to the 10th of December 2004 12.00 noon (*duration of the project*). Before the election, the election committee explained that it is a pilot project and only its success will decide on its future use. The election succeeded according to all participants and so it is planned to use it again for the election in December 2005 (*sustainability*).

Before this legally binding election there was a test election (the 30^{th} of September and the 6^{th} of October). 99 chosen GI members had the possibility to vote under the same conditions in order to test the system. These members had the possibility to return feedback. The great amount of suggestions of improvement had been realized and after that 10 of the 99 GI members had again the possibility to test the improved system (location of tests). There were many factors why the GI decided to apply e-Voting in their elections. First they write that they want to try new technologies and innovative methods. Another aim was to dispel the security doubts against electronic voting systems and the GI hoped to increase the voter turnout. Another reason to apply e-voting was the quick election results and the fact that the GI can become a precursor for other associations (aim of project).

4.1.2 Resources and Actors

In this part not many detail information is public available. The GI did not make any numbers on *budget* or *source of funding* available to the public. The same holds for *initiative*, the *actors/levels of government* and *number of agencies involved* as well as for *scientifical support and evaluation, pro and contra of actor* and *promotion*.

In the chairman election there were 20.395 eligible voters. 4.845 members cast their votes electronically and 81 persons used postal voting. So the voter turnout has been 24,2% what means that in comparison to the last chairman election in 2003 56% more GI members participated the election in 2003 (*participation and voter turnout*).

4.2 Technology

4.2.1 Postal Voting

Every GI member got a letter with the election information, briefings to use the e-Voting system, and the covered TAN code on the front. On the reverse side there was the information necessary to request postal voting material. An additional paper informed the voter about the usage of e-Voting in the GI. So if a voter preferred postal voting she had to fill out the form on the reverse side and send it back to the GI office (the postage was paid by the GI). In the next step the GI

[7] Pilot project meant that only if it works, e-Voting will become a standard solution for the future and if not, e-Voting would be dropped in favour of solely a postal voting solution

sent this voter the postal election records – a ballot, two special envelops, information about the candidates, and an additional paper for the voter's signature [12], then the user could cast her candidates and sent it back to the GI office. (*process of postal voting*).

In Germany the mail delay for letters is very short especially for national mails: 95% letters needs only one day and after two days 99% of all letters are delivered (*Failure rates of mail delivery*). Even Europe-wide 97,1 % of the letters are delivered within 3 days.

The voter's *identification* attribute within the postal voting is the voter's personal signature – as usually with postal voting in Germany. To ensure a *secret*/anonymous election, the GI election letters consists as usual out of two different envelops: the main one which consists of a paper with the voter's personal signature and voter identification attributes on it and a second envelop with the ballot inside. So identity and closed ballot envelop are separated before opening the ballot envelop. To exclude *double voting* the election record is only sent once to every voter, also if the voter complains that she has not received it or in case she cannot find it anymore. In both cases – e-Voting and postal voting – there is no special *protection against ineligible voters*. Many GI members use their office address and so they get the election records there which are not as trustworthy as those at home, because everyone in the company has access to it (Family voting becomes possible)[8].

With respect to the *protection against counting of votes before the end of the election* and the identification of fraud the GI *election committee* consists of people with different interests so they control each other. Especially they check if no ballot letter has been opened before the end of the election, because it cannot be closed again so it will be visible if some of the envelopes have already been opened.

4.2.2 e-Voting

The voters can use almost all common browsers to cast their votes without Netscape 4.7.x[9] and Lynx (*Client Software*). The infrastructure for the GI's chairman election was provided and advised by Micromata. The used severs were situated in a secure data processing service center. The whole system is based on open source software like Linux, Apache, Tomcat, Open SSL and Postgrep SQL, so it is possible to use the software in any environment (*hardware and software*).

The e-Voting software POLYAS was developed by the company Micomata Objects GmbH, which has its domicile in Kassel (Germany). The first time POLYAS was used, was in 1996 in Finland. Until now, about 250.000 voters cast their vote with this system (*developer and provider*).

The voter *identification* and authentication is based on a PIN/TAN technique. The voter uses as her PIN her membership number and her TAN is given her on the election records (under a covered field, so that no one else can read and use the TAN unnoticed). The TAN consisted on 12 characters (6212 possibilities). The main idea to ensure an *anonymous election* is the usage of pseudonyms. After the registration with a correct PIN/TAN combination, the electoral server allocates the voter to an internal ID which is called 'election token' and is later used to identify the ballot. The token is a random generated character string that is sent back to the voter (but not visible there) and in addition the election server sends it to the second election server the so called box server (but no additional information about the voter's identity). The

[8] Due to the nature of the identification form in the used e-Voting software this is an issue affecting both remote e-Voting and postal voting.

[9] The electoral page was not presented correctly with Netscape 2.7.x but never the less the voter can cast her vote with it.

allocation from the internal ID to the GI membership number on the election server is deleted immediately there and overwritten at the box server after the final ballot casting and cannot be reconstructed anymore. The only information bounded to the GI membership number at the election server is the information that this member has cast her vote electronically and that she is not allowed to cast again a ballot (*double voting protection*). Subsequently no allocation from the voter to her ballot exists, even if the attacker knows both the data from the election server and the box server. So on the one hand side the absolute separation from two servers ensures a secret and anonymous election and on the other hand side the usage of SSL for the communication between the two servers and the servers and the voter's PC. In addition to that Micromata has been committed to the German data protection principles.

With respect to *protection against ineligible* voters the difficulties are the same as with postal voting because the election record with the TAN was sent via. The POLYAS system computes continuously hash codes for the incoming ballots together with the already saved ones, so that it is impossible to manipulate the ballots later on, unnoticed, because then there is a mistake in the logical chain of the computed hash codes. In addition POLYAS provides the possibility to print the ballots in order to count the ballots again (*identification of fraud*).

The election committee is responsible for a correct election process but finally it has to trust Micromata that everything works correctly, but with Micromata and the experts we do not have people with different interests like the people on the election committee so it is not obviously that they control each other.

4.2.3 Security of e-Voting

The GI established a group of security experts to accompany the pilot election and the future process of e-Voting in the GI. This group examined the system, including the source code, the specification, and the documentation. The recommendations were realized by Micromata. The system has been checked in particular with regard to data protection and manipulations. The group consists of German university professors who are national and international known for their expertise in information security and for e-Voting and in addition e-Voting experts from the PTB (Physikalisch-Technische Bundesanstalt, Berlin): Prof. Dr. Brunnstein, Prof. Dr. Grimm, Prof. Dr. Pfitzmann, Prof. Dr. Dieter Richter, PTB Berlin (*examination, certification of the system*).

Micromata uses redundant servers to improve the system stability. In addition Micromata performed endurance testing (*load balancing*).

With respect to the *organisational surveillance of system – watchdog* we only know that the server are situated in a secure data processing service centre. There is no information available with respect to a crisis management as well as with respect to defence against DoS attacks, viruses*, and* Trojan Horses as well as against *Spoofing*, *Man-in-the-middle-attacks* and *security leaks.*

Access to the election servers is only possible for exclusive persons and in any case it is only possible if at least two persons are present. In addition every access to the server is logged and no other programs can change something according to the election software, databases or ballots because POLYAS is the only software that runs on the servers (*organizational measures against access to the servers*).

4.2.4 Outcomes

There was no special evaluation after the election, but there was a forum on the GI's web pages where people could enter their opinion. Most of the comments are positive ones (*result of evaluation*).

To the points *other outcomes, critical success factors*, and *contentedness of the voters* no information is available beside the fact that a speaker of the GI said in an interview that the election was successful and that no manipulation has been noticed.

5 Conclusion

In our analysis we assessed the level of security in remote e-Voting compared to postal voting in a multi-channel election. To compare this we developed a criteria catalogue based on previous comparative surveys in the field of e-Voting. For our assessment we selected the pilot project by the Gesellschaft für Informatik (GI) who conducted a multi-channel election offering solely remote voting channels but both electronically (remote e-Voting) and paper based (postal voting). This speciality made it very interesting to further investigate this project.

On one hand we showed that both channels share common problems in the field of secrecy of the vote in the vote casting stage is concerned. It also showed that the process of integrating multiple channels of voting results in a much higher complexity basically on the back end but not necessarily for the voter. In contrast the end users were very happy with the system which was proven by a much higher participation rate.

Overall the system used by the GI is a simple solution to a typical problem of a registered association and offers valuable information and experiences for other projects in the field of e-Voting. Still it is questionable if such a system as used by the GI would incur more problems in the field of security issues when there would massive interest of hackers in manipulating the election results. For primary elections as an election to the Bundestag one would have to use a much more advanced system – at the current level of e-Voting technology probably a kiosk system – to fully guarantee the legal election principles but one can definitely profit from the experiences made with the GI elections.

References

[1] Prosser, A., Krimmer, R.: Electronic Voting in Europe. ESF TED Conference Bregenz, GI, Bonn, 2004.

[2] 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

[3] Macintosh, A.: WG4 report to the European Commission, Brussels, 2003. Available at `http://www.eu-forum.org/summit/docs/WG4e-democracy-FINAL\%20RESULTS.docaccessedon2005-03-05`.

[4] Braun, N., Prosser, A., Krimmer, R.: Braun, N., Prosser, A., Krimmer, R.: Öffentliche Wahlen im Internet: Ein Vergleich zwischen der Schweiz und Österreich, In: Wimmer, M.: Proceedings of the 2nd E-Gov Day, Vienna, 2003.

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

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

[7] Prosser, A., Krimmer, R.: The Dimensions of Electronic Voting. In: Prosser, A. Krimmer, R.: Electronic Voting in Europe. ESF TED Conference Bregenz, GI Verlag, Bonn, 2004.

[8] Wählen auf Distanz: Ein Vergleich zwischen elektronischem und nicht-elektronischem Verfahren. Will appears in: Schweighofer, Menzel, Liebwald: IRIS 2005.

[9] Bundesministerium der Justiz: Bürgerliches Gesetzbuch, 2002-01-02 . Available at http://bundesrecht.juris.de/bundesrecht/bgb/ accessed on 2005-03-09.

[10] Gesellschaft für Informatik: Satzung der Gesellschaft für Informatik, Bonn, 2003-07-21. Available at `http://www.gi-ev.de/verein/struktur/satzung.shtml` accessed on 2005-03-09.

[11] Gesellschaft für Informatik: Wahlordnung der Gesellschaft für Informatik Version vom 2004-09-21, Bonn,. Available at `http://www.gi-ev.de/verein/struktur/wahlordnung.shtml` accessed on 2005-03-09.

[12] Initiative D21, Onlinewahl, `http://www.initiatived21.de/online-wahlen` accessed on 2005-03.09.

[13] Mausch, M.: Mobile Fusion, Mimori Group, `http://www.mimori-group.com/obj/Dokumente/Mobile_Fusion.pdf` accessed on 2005-03-09.

[14] Gesellschaft für Informatik: Wahlunterlagen für die Präsidiumswahl 2004, Bonn.

[15] Micromata Objects GmbH, System Polyas. Information available at `http://www.micromata.de/M_tech/wahl/content.html` accessed on 2005-03-10

[16] Gesellschaft für Informatik: Gesellschaft für Informatik hat Onlinewahl erfolgreich erprobt Available at `http://www.gi-ev.de/informatik/presse/presse_041210.shtml` accessed on 2005-03-10

[17] Gesellschaft für Informatik: FAQ-Liste zur elektronischen Wahl 2004, Bonn. Available at `http://www.gi-ev.de/praesidiumswahl2004/pwahl_faq.shtml` accessed on 2005-03-10

[18] Heise online: Gesellschaft für Informatik wählte Präsidium erstmals online. Available at `http://www.heise.de/newsticker/meldung/54204` accessed on 2005-03-10

[19] Elektronikbranche.de: Größte rechtsverbindliche Online-Wahl in Deutschland ein voller Erfolg, Kassel. Available at `http://www.elektronikbranche.de/index_na_anz.html` accessed on 2005-03-10

[20] IT SecCity, Micromata Henkel, T.: Micromata: Größte Online-Wahl in Deutschland ein voller Erfolg – GI wählt mit POLYAS rechtsverbindlich ihr Präsidium, 2004-12-29. Available at `http://www.itseccity.de/?url=/content/markt/nachrichten/041229_mar_nac_micromata.html` accessed on 2005-03-10

[21] Bundesverband Deutscher Postdienstleister e.V.: Deutsche Post bei Brieflaufzeiten Spitze in Europa, 2005-02-11. Available at `http://www.bvdp.de/index.htm?/files/briefe-kep/349391D52AA64F098289700464726A8B.htm` accessed on 2005-03-15

[22] Int. Post Corp.: External Quality of Service Monitoring – Improving the Quality of Int. Mail – Results 2004. Available at `http://www.ipc.be/documents/2004_UNEX_Results.pdf` accessed on 2005-03-15