A Security Analysis of the Swiss Electronic Voting System

Author: Andrea Baumann  
05-533-971

Author: Daniela Häberli  
08-211-666

Department: Department of Informatics, University of Fribourg

Course: Electronic Government

Examiner: Prof. Andreas Meier

Supervisor: Luis Terán

Date: December 1, 2013
Executive Summary

The implementation of the e-voting system in Switzerland caused concerns about different security issues. Since the start of the pilot project, there are controversial discussions. Whereas e-voting supporter have the hope of positive effects such as higher voter participation, enhanced pre-electoral opinion formation, or enhanced cost-effectiveness, critics have high concerns about the security of e-voting systems.

The aim of this thesis was to analyze the security of the Swiss e-voting system and to find risks regarding e-voting. Moreover, the perception of the security of citizens should be evaluated, to gain an impression of the trust of people.

The results of the thesis found that the security awareness is very different. While the advocate of the system argue that the security requirements are almost fulfilled, due to the implementation of the verifiability, the critic has high concerns about e-voting systems. The counterparts agree about the existence of risks, but they disagree about the seriousness. Whereas the trust of citizens is generally rather high, in this thesis questionable security aspects were found.

In case of a definitive implementation of an e-voting system, it has to be secure without vulnerabilities. Therefore to evaluate the system, criteria for an absolute secure system are used (Accuracy, Democracy, Privacy, Verifiability, Fairness). To do the evaluation, two interviews are realized with an advocate and a critic of the e-voting system. The perception of citizens is analyzed based on a social survey.

The authors have doubts, if the effort for implementing an e-voting system is justified, because it is questionable if in the next years solution to face all the risks can be found. Furthermore, the authors insist that today with the paper voting a secure, prompt and inexpensive voting system already exists.

Key words: eGovernment, eDemocracy, e-Voting, Security, Risks
# Table of Content

Executive Summary ............................................................................................................. I

Table of Content .................................................................................................................. II

List of Figures ...................................................................................................................... IV

1 Introduction ...................................................................................................................... 5
   1.1 Objectives .................................................................................................................. 5
   1.2 Background and Problem Statement ........................................................................ 6
   1.3 Research Question ...................................................................................................... 7
   1.4 Methodology ............................................................................................................... 7

2 Foundations ...................................................................................................................... 8
   2.1 Definition and Aims of E-Voting ................................................................................ 8
   2.2 Existing Systems in Switzerland .............................................................................. 9
   2.3 Lessons learned .......................................................................................................... 10

3 Security Requirements ..................................................................................................... 11
   3.1 Definition Accuracy ................................................................................................... 11
   3.2 Definition Democracy ............................................................................................... 12
   3.3 Definition Privacy ..................................................................................................... 12
   3.4 Definition Verifiability .............................................................................................. 12
   3.5 Definition Fairness .................................................................................................... 13

4 Evaluation of the E-Voting System .................................................................................. 13
   4.1 Evaluation Accuracy .................................................................................................. 13
      4.1.1 Survey Mr. Langenauer .................................................................................... 13
      4.1.2 Survey Mr. Ragaz ............................................................................................. 14
   4.2 Evaluation Democracy ............................................................................................... 14
      4.2.1 Survey Mr. Langenauer .................................................................................... 14
      4.2.2 Survey Mr. Ragaz ............................................................................................. 15
   4.3 Evaluation Privacy ..................................................................................................... 15
      4.3.1 Survey Mr. Langenauer .................................................................................... 15
      4.3.2 Survey Mr. Ragaz ............................................................................................. 15
   4.4 Evaluation Verifiability ............................................................................................... 16
      4.4.1 Survey Mr. Langenauer .................................................................................... 16
      4.4.2 Survey Mr. Ragaz ............................................................................................. 16
List of Figures

Fig. 1: Evaluation of the Interviews ................................................................. 18
Fig. 2: Risk matrix after Mr. Langenauer and Mr. Ragaz ................................. 24
Fig. 3: Do you have concerns about e-voting? ............................................... 25
Fig. 4: Do you have concerns about the electoral freedom? ......................... 25
Fig. 5: Do you have concerns about the accountability of the voting process? .... 26
Fig. 6: Do you have concerns about the correctness of the voting result? ......... 26
Fig. 7: Do you have concerns about the guarantee of the secrecy of the ballot? ..... 27
1 Introduction

This seminar thesis is for the lecture Electronic Government at the University of Fribourg. Students were asked to choose between three types of project possibilities: Research Paper Study, Study Case or Prototype. This paper focuses on a Study Case in the range of e-voting. The thesis is structured as follows: Firstly, the Objectives, the Problem Statement, the Research Questions and the Methodology are defined. Secondly, some explanation regarding the existing e-voting systems in Switzerland are mentioned, which are followed by the definition of the security requirements. In addition, the evaluation of the Swiss e-voting system is done based on two interviews and a survey. Finally, an overview of the risks is given in a risk matrix.

The thesis focus on the e-voting system of Zurich, due to the fact that one interview partner is responsible for the e-voting project in the Canton of Zurich. Nevertheless, to have the whole context, in the first parts the Swiss e-voting project is also taken into consideration.

1.1 Objectives

The implementation of the e-voting system caused concerns about different security issues. Since the start of the pilot project, there are controversial discussions.

The objective of this thesis is to analyze how secure the Swiss e-voting system is. Based on criteria for a secure system, lacks of security will be displayed to point out where improvements of the system are necessary to guarantee a reliable ballot.

Another objective is to analyze if there is any gap between the real and the perceived security. This is relevant because trust plays an important role when executing the political rights in Switzerland (Bericht des Bundesrates, 2013, p. 85).
1.2 Background and Problem Statement

The “information and communication technology” (ICT) record a fast development. In Switzerland not only the private sector but also the public and political institutions are influenced by ICT.

E-voting supporter has the hope of positive effects such as higher voter participation, enhanced pre-electoral opinion formation, or enhanced cost-effectiveness (Haenni; Dubuis, 2008, p. 2).

The federal, cantonal and communal authorities and also politicians as parties do more and more use the internet for sharing information with the public. According to that circumstance, it can be thought to think about the execution of political rights through electronic procedures. This could be a new chance for our democratic system. In Switzerland the pilot project “Vote électronique” (e-voting) exists already since the year 2000 and is in development since then. The federal council got the mandate from the parliament to introduce a voting system incremental (Bericht des Bundesrates, 2013).

A gap of security could be a threat to democracy. Therefore high security standards have to be met to avoid risks and guarantee smooth democratic functions. The gradual introduction is a consequence and follows the principle “security before velocity”. Due to the fact that Switzerland has one of the most improved e-voting systems, not much comparison and adaptation can be done to find and overcome security concerns (Bericht des Bundesrates, 2013).

Rivals of the project criticize its security and mention different issues. The argument most frequently used is that “e-voting is fundamentally insecure” (Simons; Douglas, 2012, p. 68) because different kind of manipulation is possible. Further they state that a result, which has been manipulated, cannot be recounted properly. There are also doubts about the guarantee of the secrecy of the ballot (VPR 27g Abs.1). Another argument used is the questionable validity of the pilot project. Meaning that either the system was not hacked because of the low interest to manipulate a pilot project or the manipulation was not recognized. Therefor from opponents the e-voting system is seen as a “possible threat to democracy” (Ragaz, 2013, NZZ).
1.3 Research Question

The following research questions are answered in the actual case study:

- What are characteristics of a secure e-voting system?
- How are the different criteria evaluated at the Swiss e-voting system?
- What are the risks of the e-voting system?

1.4 Methodology

To find characteristics of a secure e-voting System, research papers were analyzed. In case of a definitive implementation of an e-voting system, it has to be secure without vulnerabilities. Haenni and Dubuis, 2008 mentioned that the launch should be allowed through a secure design. Although the complexity of the design and implementation of such a system, “some criteria seem to be unanimously accepted as the core security requirements for e-voting” (Haenni; Dubuis, 2008, p. 2). They used five criteria in their research paper, which has to be fulfilled to achieve a secure system. These security requirements are: Accuracy, Democracy, Privacy, Verifiability and Fairness. The evaluation is based on this five criteria.

This criteria are used because they include the principles governing the law of elections (Wahlrechtsgrundsätze), which are of prime importance for implementing an e-voting system. Therefore they are more specific for e-voting than criteria used in other papers. Moreover, the verifiability, described in part three, is of a wide consensus in the literature about the importance of this property.

Other security criteria for an e-voting system are proposed by Neumann, 1993. In his paper he uses, beside other criteria, availability, reliability, accountability, auditability, disclosability and transparency as system requirements. This characteristics are more generally for a secure system (Neumann, 1993).

Fujioka et al., 1993 defines seven requirements of a secure voting system: completeness, soundness, privacy, unreusability, eligibility, fairness, verifiability, which are basically identical to the criteria used in this paper (Fujioka et al., 1993).
For this Study case two interviews were realized based on the already mentioned five criteria. Those interviews are done with two experts, where one is pro and the other contra to the e-voting system:

- Stefan Langenauer who is Head of the “Statistischs Amt des Kantons Zürich” and is responsible for the e-voting project in the Canton of Zurich. The interview took place in Zurich at November 15, 2013.
- Niklaus Ragaz who is a Former Head of the „Amt für Informatik des Kantons Bern“, CEO of the „Bedag Informatik“ and was Honorary Professor for „Wirtschaftsinformatik“ at the University of Berne. He is a critic of e-voting over the Internet. The interview took place in Lugano at November 19, 2013.

In addition, a social survey was done with 20 participants to evaluate how citizens perceive the security of the e-voting system. Ten of them already had experience with the e-voting system.

The output of this two interviews and the survey is used for the evaluation of the security side of the e-voting system in Switzerland. Moreover, a risk matrix will be shown, that illustrates the general risks of e-voting.

2 Foundations

2.1 Definition and Aims of E-Voting

The Swiss Federal Council adopted 2007 the E-Government-Strategy of Switzerland. This strategy has the target that economy and the Swiss population should be able to conclude all important business with the authorities through an electronic system. Whereby the “Vote électronique” should be prioritized (Bericht des Bundesrates, 2013, p.2).

After the “Competence Centre for E-voting and Participation” e-voting or electronic voting, in a broad sense, is the employment of ICT in one of the following processes: Identification of the voter, casting of the vote and counting of the vote. In a more narrow sense, e-voting is the use of information and communication technology at least at the disposal of the vote (Competence Centre, 2013).
In the following thesis, e-voting is used as the possibility of casting the vote on the Internet. Another term for Internet voting is remote electronic voting. In Switzerland, a project to introduce text messages for casting the vote is stopped after being tested in the pilot project (Competence Centre, 2013).

“Vote électronique” is a project in Switzerland from the federation and the cantons. This should transfer the culture and tradition of the political system in the technologies of the 21st century. The requirement on mobility has increased over the last decades and brought up a general change in the democratic instruments. After the launch of a few other systems, such as online-banking and tax declaration, the introduction of an online voting system is a logical consequence. E-voting is an investment of federation and cantons and should guarantee a quality improvement. Especially is the system an improvement for eligible voters, which are visually impaired or Swiss expats (Bericht des Bundesrates, 2013, p. 2).

Following a first report in the year 2002 about the feasibility, the strength and the risks of e-voting, it came the first pilot project. It was launched in three cantons: Zurich, Neuchatel and Geneva. The second report in 2006 included a positive evaluation of the pilot project, which took place between 2004 and 2005. On January the 1, 2008 the legislation amendment was adopted, which was necessary for an additional pilot stage, which is still on going. The change of the legal basis enables the implementation of e-voting into the cantons. The modification concerns the federal law (Bundesgesetz) regarding the political rights (included also the political rights from Swiss expats) and the regulation (Verordnung). It creates a controlled expansion of the e-voting system into other cantons. Today around ten percent are permitted to use e-voting in Switzerland (Bericht des Bundesrates, 2013, p.2).

2.2 Existing Systems in Switzerland

Pilot project 2005-2007
The e-voting system from the canton of Zurich was first tested in the communities Bülach, Schlieren and Bertschikon. Base on the Swiss national referendum from November 27, 2005 and November 26, 2006 and June 17, 2007 it was successfully used (Kanton Zürich, 2013).
**Trial phase 2008-2011**

The communities Mettmenstetten, Kleinandelfingen, Boppelsen, Bubikon, Thalwil, Männedorf, Fehraltorf, Mauer and the old city of Winterthur as well the first and second district of the Zurich city also joined the trial phase from 2008 to 2011 (Kanton Zürich, 2013):

- 2008: expansion of the e-voting test to approximately 66'000 eligible voters (without city of Zurich) on the September 28, 2008
- 2008: expansion of the e-voting test to approximately 89'000 eligible voters (all enlisted communities and city district) on the November 30, 2008
- 2009: e-voting is in action on all the official election dates and with all the involved communities and city districts
- 2010: Inclusion of the Swiss expats from the city district (e-voting trial on the September 26, 2010

**Outlook**

The “Statistical Department of the Canton of Zurich” prepared a closing report regarding the e-voting trial phase 2008-2011. In the November 2011 the governing council (Regierungsrat) of the Canton of Zurich has based on this closing report and the inputs of the Swiss Federal Council and therefore decided how the e-voting system will be implemented in the Canton of Zurich after 2012 (Kanton Zürich, 2013).

**2.3 Lessons learned**

As mentioned before, today 10 percent of the Swiss electorate is entitled to vote electronic (VPR). In 2012, the confederation came to the conclusion that today’s e-voting systems fulfill the security requirements defined in the VRP, if the limit of 10 percent is not increased. But it was decided that today’s security standards are not sufficient for a bigger electorate. Therefore, an increase of the limit is only possible on condition that the newly defined security requirements are implemented (Bericht des Bundesrates, 2013, p. 104).

A system that fulfills the newly defined security requirements, is known as a „second generation system“ and allow 100 percent of the Swiss electorate to vote electronic (Bericht des Bundesrates, 2013, p. 119). Especially, the verifiability (see 3.4) is part of the new requirements. It guarantees that systematic defective functions, due to
software error, human mistake or intentional manipulation, while protecting the secrecy of the ballot, are recognized (Bericht des Bundesrates, 2013, p. 115). Because the development of a second generation system is time-consuming and creates high costs, a reduced form of the verifiability is accepted to increase the limit to 50 percent of the electorate (Bericht des Bundesrates, 2013, p. 119).

To meet these requirements the system has to guarantee that a voter can verify if his vote is casted as intended. This measure solves the problem of the unsecure user platform to a great extent (Bericht des Bundesrates, 2013, p. 120). Not necessarily does the system have to verify if a vote is recorded as a cast and is counted as recorded. These requirements are planned to be implemented in the long-term.

3 Security Requirements

Voting is a core element of the democratic system. A voting system has to function without vulnerabilities to preserve citizens trust. Compared to the conventional voting, the electronic voting system operates in the potential unsecure environment of the Internet. Due to the centralization of the electronic urn and the associated possibility that the whole urn can be befallen, there is a higher risk for large-scale attacks. The implication is a security-critical system, which has to meet the highest possible security measures.

The criteria used in this thesis to evaluate the Swiss e-voting system, as described in 1.4, are proposed from Haenni and Dubuis, 2008 as requirements for a secure system. They describe the ideal case of an absolute secure system, which in practice should be an as close approximation as possible.

The following definitions are based on Haenni and Dubuis, 2008 and Dubuis, Haenni and Koenig, 2012:

3.1 Definition Accuracy

The determination of the correct result is a general requirement for a voting system. Concerning e-voting, the accuracy aims to the avoidance of manipulation. It must be guaranteed that no voting result is accepted that does not reflect the collective will of
the constituents. In detail accuracy is meet if the casted votes cannot be altered or replaced on the way to the electronic urn, if all valid votes are counted and invalid votes are not counted.

### 3.2 Definition Democracy

The voting process is democratic if the eligibility is proved and authorized voters can only vote once.

### 3.3 Definition Privacy

The secrecy of the ballot is based on the “Verordnung über die politischen Rechte” (VRP Art. 27g and Art. 27h). It gives the voters the right to vote secretly and without any pressure from outside. This implies that no link between the casted votes and its voters can be made and the detection if somebody voted or not is impossible. Furthermore the principle of receipt-freeness guarantees that voters cannot prove that they voted in a particular way.

### 3.4 Definition Verifiability

In contrast to the conventional voting, an e-voting system is very complex and hardly comprehensible for the wide public due to the technical design. To improve citizens trust, a procedure is implemented to verify the correctness of the result according to the accuracy as described above. The verifiability can be divided into two parts: the individual and the universal verifiability.

The individual verifiability contains the possibility for a voter to verify his vote on the result. A voter can review if his vote is casted as intended, recorded as a cast and is counted as recorded. With the universal verifiability voters can verify independently that all valid votes are counted correctly. But the secrecy of the ballot must not be violated.

To implement both the individual and the universal verifiability, scientists are developing advanced cryptologic methods. To apply the verifiability to the e-voting system, after casting the vote, codes will be displayed which serves that voters can verify the correctness of their vote.
3.5 Definition Fairness

For a fair ballot early results must not be available during and after the voting process. This avoids mobilization of voters in the last moment and therefore the possibility to influence the voting result.

4 Evaluation of the E-Voting System

For each criteria, the “scaled question” is shown and is followed by the answers from the interviews. The scale, which is used in the interviews is: “Not fulfilled”, “slightly fulfilled”, “partly fulfilled”, “fulfilled” and “I don't know” (see the whole questionnaire in the Appendix). The two interviewee are referring to the second generation system, as described in 2.3.

Mr. Ragaz mentioned, that concerning e-voting not a particular system is insecure but that there are risks lying in the environment and making e-voting generally insecure. Therefore the risks cannot be assigned to one of the five criteria but has an influence on every of them. The risks are explained in detail in Chapter five.

4.1 Evaluation Accuracy

<table>
<thead>
<tr>
<th>Scaled questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system guarantee...</td>
</tr>
<tr>
<td>a) ...that the casted votes can not be altered or replaced?</td>
</tr>
<tr>
<td>b) ...that all valid votes are counted?</td>
</tr>
<tr>
<td>c) ...that invalid votes are not counted?</td>
</tr>
</tbody>
</table>

4.1.1 Survey Mr. Langenauer

Mr. Langenauer answered, that the casted votes could be only delivered once. In the beginning, the voters cast their votes and save them. After that, the votes cannot be either altered or replaced. Afterwards, the casted votes will be verified with codes before they go directly to the urn. According to Mr. Langenauer, the system with the verifiability (which is mentioned later) makes a replacement of the vote impossible. He also answered the second question with “fulfilled” because he argued, there are only valid votes because of the “log-in” system. This already answered also the last
question; invalid votes do not exist. An error report would appear (last question is also “fulfilled”).

According to Mr. Langenauer the above-mentioned criteria are all technically ensured. He sees the risk that the confidence of the people could be lost if something occur. But this probability is very low after him.

**4.1.2 Survey Mr. Ragaz**

Mr. Ragaz argued that due to the risks, which are described in Chapter five, such as an attack on the server or the impersonating of the election server, casted votes could be manipulated. Therefore he stated that the system does not necessarily guarantee that casted votes cannot be altered or replaced and therefore it is not technically ensured. The voting on a counterfeited website has the consequence that a casted vote does not reach the electronic urn. That is why he also answered the second question with „not fulfilled“. The same answer he gave at the last question, because by virtue of manipulation invalid votes are possible.

He insisted on the point that, whereas at the postal voting a large group of people need to work together to do a large-scale manipulation, in the e-voting system a single person can alter a high number of votes.

**4.2 Evaluation Democracy**

<table>
<thead>
<tr>
<th>Scaled questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system guarantee...</td>
</tr>
<tr>
<td>a) ...that the eligibility is proved?</td>
</tr>
<tr>
<td>b) ...that authorized voters can only vote once?</td>
</tr>
</tbody>
</table>

**4.2.1 Survey Mr. Langenauer**

In the next two questions of the survey, Mr. Langenauer has not seen any differentiation to the conventional voting (which means voting by paper). This means that he answered both questions with “fulfilled”.
According to him, the risk is similar to the conventional voting system because it is also possible to intercept the voting papers, which arrives postal. After him the probability is low, also the impact would be low since it only concerns individual votes and not big amount of voting numbers.

### 4.2.2 Survey Mr. Ragaz

Referring to the risks mentioned further down, the system does not necessarily guarantee that only eligible voters can vote. An example is phishing, whereby secret identification information can be collected to vote instead of an eligible voter. Therefore, Mr. Ragaz stated that the first question is “not fulfilled”. The second question is “partly fulfilled” because the possibility that a voter deliver its vote twice is small and also the impact is minimal.

### 4.3 Evaluation Privacy

<table>
<thead>
<tr>
<th>Scaled questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system guarantee...</td>
</tr>
<tr>
<td>a) ...that casted votes can not be linked to its voters?</td>
</tr>
<tr>
<td>b) ...that no detection of citizens who voted/did not vote is possible?</td>
</tr>
<tr>
<td>c) ...that voters can not prove that they voted in a particular way?</td>
</tr>
</tbody>
</table>

#### 4.3.1 Survey Mr. Langenauer

According to Mr. Langenauer, the link between casted votes and voters is not possible. Also the detection of citizens who voted or not, is not possible. Hence, the system guarantees that it is not understandable if people vote in a particular way.

He ticked all the questions with “fulfilled” and is convinced that the secrecy of ballot is not vulnerable. The impact of breaking the law would definitely be enormous, but almost impossible assured by the safe system.

#### 4.3.2 Survey Mr. Ragaz

As Mr. Ragaz does not know the specific implementation of the e-voting system of Zurich, he cannot answer the first question for sure. The second question he an-
answered with “not fulfilled“ due to the possibility to direct voters on a counterfeited website, then seeing how certain voters intended to vote. Concerning the third question, he stated that depending on how the verifiability is implemented, one can possibly confirm how he voted. Moreover, with malware on a voters PC, one can detect how a particular voter give his voted. Therefore this question he answered with „not fulfilled“.

4.4 Evaluation Verifiability

<table>
<thead>
<tr>
<th>Scaled questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Is the individual verifiability given? (voters can verify that their vote is casted as intended, recorded as a cast and is counted as recorded)</td>
</tr>
<tr>
<td>b) Is the universal verifiability given? (voters can verify independently that all valid votes are counted correctly)</td>
</tr>
</tbody>
</table>

4.4.1 Survey Mr. Langenauer

The individual verifiability is one of the most important improvements in the second generation system, according to Mr. Langenauer. The scaled question is fulfilled in the survey. The universal verifiability is not implemented yet. It is expected to be implemented in 2017 or 2018.

Mr. Langenauer argues that the risk of manipulation is very small due to the fact that the verifiability is mathematically proven. In addition during the voting process the individual has to enter passwords and codes several times.

4.4.2 Survey Mr. Ragaz

Mr. Ragaz stated that to introduce the verifiability in the e-voting system is a slight improvement. But he mentioned that security issues are often binary. Meaning that security is “not partly” or “slightly fulfilled”, either it is “fulfilled” or not. He said that one can prove mathematically that systems with the verifiability are secure, but only theoretically. The verifiability does not solve the problem of phishing, denial-of-service attacks or attacks on the server.
The phishing issue he explained with an example from Norway. An experiment was designed to test with college and high school students if the verifiability work as desired. But they came to another result. With an additional question they reached to collect the secret party codes from all the students, despite showing an animation, which emphasized on the correct use of the party code. None of the students found any faults with the system. After collecting the code they could easily send the right confirmation code (Olsen; Nordhaug, 2012, p.37). Therefore he mentioned that the verifiability is only secure if voters do what they are supposed to do.

Moreover, he insisted on the point that the verifiability does not solve the problem of a hacker attack on the server. Even if voters verify their votes, they can later be manipulated on the server. And nobody will recognize it. Here he mentioned that the verifiability has two vulnerabilities. If on the server the votes are stored so that a link can be made to the voter, the secrecy of the ballot is violated. If votes are stored independent of the voter, a hacker can manipulate the votes without recognition. And therefore even the universal verifiability cannot solve this problem.

He also referred to an article in the newspaper Neue Zürcher Zeitung (Baumgartner, 2013), where Mr. Birk stated that the method of the verifiability is not feasible. If complicated codes have to be entered or verified, the acceptance of the voters is ignored.

Consequently, he answered that the individual and the universal verifiability are not fulfilled.

4.5 Evaluation Fairness

<table>
<thead>
<tr>
<th>Scaled questions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system guarantee...</td>
</tr>
<tr>
<td>a) ...that no early results are available during the voting process?</td>
</tr>
<tr>
<td>b) ...that no early results are available after the voting process?</td>
</tr>
</tbody>
</table>
4.5.1 Survey Mr. Langenauer

It is technically ensured that early results are not possible to obtain. In addition, he argues that regarding fairness, the e-voting system is much more fair than the conventional one.

4.5.2 Survey Mr. Ragaz

Mr. Ragaz mentioned that if a hacker succeeds in penetrating the server, he can determine early results and also make them available after the voting process. Therefore both questions are not fulfilled.

4.6 Conclusion

To summarize the interviews, it can be stated that the two experts do have contrary opinion regarding the security of the e-voting system; showed by the graphic bellow (Fig. 1).

![Evaluation of the Interviews]

Fig. 1: Evaluation of the Interviews

1 Not fulfilled; 2 Slightly fulfilled; 3 Partly fulfilled; 4 Fulfilled
5 Risks of E-Voting

Through the interviews several risk were found, which are described in the first part bellow. The second part shows a risk matrix according to the answers of Mr. Langenauer and Mr. Ragaz.

5.1 Risks

What follows is a list of the main risks Mr. Langenauer and Mr. Ragaz mentioned. The different risks are described and examples are given.

For the technical risks, Mr. Ragaz was referring to two articles „Internet Voting in the U.S“, (Simons; Douglas, October 2012) and „Internet Elections: Unsafe in Any Home?“, (Olsen; Nordhaug, August 2012 from the journal „Communications of the ACM“).

5.1.1 Loss of trust

Mr. Langenauer sees a high risk that the confidence of the people could be lost if something occur. Due to the fact that trust is the basis for smooth democratic functions. But this probability is very low after him.

5.1.2 The server attack

The server consists of the operating system, the application and the data. Here the operating system is the vulnerable part. As Mr. Ragaz mentioned, if a hacker can enter the server, he is able to manipulate votes. Compared to the conventional voting system where a large-scale attack is difficult to realize, in the e-voting system a single person has the possibility to manipulated a high number of votes. “Independent hackers, political operatives, foreign governments, and terrorists could amount such attacks” (Simons; Douglas, 2012, p. 68). And this from all over the world.

To illustrate the vulnerability of the server, Mr. Ragaz mentioned that, despite large security precautions, major corporations as banks, governments and pharmaceutical companies have been attacked successfully. In contrast to Mr. Langenauer, Mr. Ragaz states that such corporations have fare more security expertise and more re-
sources. And therefore it is an illusion to think that an e-voting project can attain higher security standards.

At last, he insisted that manipulation is such a big problem because if performed well, no detection is possible. And even the verifiability, as described in part 3.4, cannot solve this problem.

According to Mr. Langenauer, the possibility that a ballot or the server is attacked is little. He compared the voting system with the “online banking” where usually a financial compensation for the individual is made. He argued that there are also few attacks on the online banking. The impact if the voting system would be hacked would be enormous and a big issue for the reputation.

5.1.3 Insider attacks

The risk when using e-voting is that an insider, like a programmer or an election official, could manipulate the voting result. Mr. Ragaz stated that this is possible due to the fact that a programmer knows every detail of the software. In contrast to the conventional voting system, where no single person can decode the urn, this is possible in the e-voting system.

One possibility is to add a “back door” to the system and as Mr. Ragaz mentioned there is few chance of detection. It could be an act of revenge from an ex-employee or also being done under coercion. Furthermore, he emphasized that the risk of insider attacks should not be underestimated.

A solution proposed from election officials, to prove the security of the e-voting system, is to publish the source code. Then it could be verified from independent experts. A critique, which is presented by Mr. Ragaz, is that it would be very hard to verify that the running system really is based on the published source code. An insider could have changed it beforehand. Additionally, this could be a clue for an inside attacker.

According to Mr. Langenauer, the risk of an insider attack is the biggest issue. The probability he argues is low, because organizational action has to be taken to face
this problem. Examples are that the four eyes principle has to be expanded to more people and that the composition of people changes, who decode the electronic urn. The impact he sees as high.

5.1.4 The client

Similar to the server, the personal computer consists of the operating system, the presentation and the e-voting application. Again the operating system is the vulnerable part, additionally to the insecurity of the browser. Mr. Ragaz argues that Malware can infect the PC’s linked to the Internet with simplicity because this happens without the knowledge and the permission of the owner. Examples of malware are viruses, worms or Trojan horses. Ways to infect PC’s are numerous and once installed the malware can steal the credential, copy the ballot to a third party, modify the vote before encryption or prevent the voting. Therefore Mr. Ragaz is seeing this risk as the most significant.

Mr. Langenauer agreed that a PC can be infected with Malware. But he stated that only a minority of voters would be affected. Compared to the entity of voters this would be only a small part. Therefore, the impact does he sees as low. The probability is medium.

Mr. Ragaz mentioned that nowadays receiving a long list of selected email addresses is easy. Then you have the possibility to contact voters with a certain profile, for example sympathizer of the green party, adding an attachment that infects the PC immediately with malware if opened. Once installed the malware can take complete control of the compromised system. Due to the ignorance of most citizens, how to protect their PC’s sufficiently, the operating systems of privates are so vulnerable.

To face the problem of the insecure user platform, in the long-term, the persons responsible of the e-voting project try to introduce an appliance for the voting, similar to e-banking. Voters log in with this appliance and give their votes. It serves the undeniable identification and the impossibility to insert malware, but as Mr. Ragaz commented, it does not solve the problem of the later manipulation of votes. Manipulation on the server is still possible and the expenditure therefore unreasonable.
5.1.5 Impersonating the election server

One possibility to impersonate the election server is spoofing. Counterfeited websites can be made that they look like legitimate sites. So that voters think they have actually voted, when their vote never reached the electronic urn. Moreover, with spoofing authentication codes or information about how voters intended to vote can be collected.

Phishing is being used to steal personal information with emails that impersonate coming from the official voting office, or that voters cast their votes on a false URL. When such emails or websites are well designed, voters will not notice that they are counterfeited.

Mr. Ragaz referred to the above-mentioned experiment with college and high school students, which can be called „digital natives“. In this experiment secret codes could be collected from students despite emphasizing on the correct use of the party code. After fishing the secret codes it was easy to send the right confirmation code. None of the students found any default with the system.

According to Mr. Langenauer, the risk of phishing is very low because it should be found out through the voter itself, if receiving no or a false code.

5.1.6 Denial-of-service attacks (DOS-Attack)

Concerning e-voting, a denial-of-service is the unavailability of the voting service. By sending a high number of requests to the Internet access or to the operating system, or more efficient, by inducing an error function when taking advantage of a program error, the voting service can be taken intentionally out of service. Consequently, the voters temporary cannot cast their votes electronically.

There are many instances of denial-of-service-attacks, examples are attacks on Google, Twitter, Facebook and WikiLeaks. Also politically motivated attacks have become relatively common. Moreover, Mr. Ragaz referred to the possibility to buy such attacks from cyber-criminals.
It exists two possibilities to do a denial-of-service-attack. One possibility is to prevent certain groups from voting. An example Mr. Ragaz mentioned is that certain districts could be brought to a standstill. The share of voters who vote right or left differs from district to district, so that an attack on a certain quarter can prevent either right or left voting citizens from voting. Another possibility is to disrupt the entire election by attacking the election server.

Mr. Ragaz came up with the question what would be done if such attacks occur. Is this a reason for an election rerun?

Mr. Langenauer argued that if an attack occurs, the electronic urn is open long enough that citizens can try again to cast their vote. Additionally, they can still use the postal vote or can go to the polls, as the electronic voting system is an alternative to the conventional voting system and will not replace it.

### 5.1.7 Bribery

Mr. Ragaz stated that in contrast to the conventional voting, the risk of manipulation for e-voting is bigger because coercion is possible. The bribery can lead to an insider attack, manipulation of votes or a denial-of-service attack.

An example mentioned by Mr. Ragaz is from the U.S., where a team from the University of Michigan could enter the e-voting pilot project in Washington in 2010 and thereby gaining almost total control over the server. The leader of the team later said that the attack would have cost less than $50'000, calculated with generous consulting rates. Compared to the expenditures for voting campaigns, this would be a small fraction of the costs.

### 5.2 Risk matrix

After discussing the risks of e-voting with Mr. Langenauer and Mr. Ragaz, they were asked how they perceive the probability of occurrence and the impact of the different risks. Accordingly, the risks were placed in the risk matrix (Fig. 2).
Mr. Ragaz stated that for the bribery the impact is high, but he could not quantify the probability.

6 Evaluation of the Social Survey

Beside the Interviews with the two experts, 20 people were asked to participate a survey for this case study. The aim was to analyze how citizens perceive the security of the e-voting system and if any, what kind of concerns they have. This is relevant because trust plays an important role when executing the political rights in Switzerland (Bericht des Bundesrates, 2013, p. 85) due to the fact that a voting system is the basis for a democracy. Therefore trust guarantees smooth democratic functions. Moreover, out of the 20 people 10 already had experience with e-voting. The question was, if there is any difference in the perception of people who already used e-voting and such who did not. To have an unambiguous analysis, a scale with an even number is used (see the whole survey in the Appendix).

6.1 Results of the Social Survey

First, it can be stated that when people were asked if they have concerns about the security of e-voting, 80 percent have very small or rather small doubts and only 20
percent have rather big or very big concerns. The majority of people have rather small doubts (Fig. 3). Surprisingly, this result is independent of the age. Fifty percent of people who have rather big or very big concerns are from 26 to 35 years old, 25 percent each 36 to 45 and over 65. Further no typological structure could be found of people who generally distrust the Internet. Nearly all of the people who have rather big or very big concerns do use the Internet for e-banking and e-commerce.

Interestingly, it could be found that those questioned who already have experience with e-voting have far more doubts about the security of e-voting than people with no experience. Seventy-five percent of those with rather big or very big concerns indicated to have already used e-voting.

When asking people what kind of concerns they have about e-voting, it is found that all of those questioned have either very small or rather small doubts about the electoral freedom. The majority of people, 75 percent, have very small concerns, meaning that corruption or bribery is scarcely conceivable (Fig. 4).
It can be thought that due to the high complexity of an e-voting system, citizens have concerns about the accountability of the voting process. It turned out that the vast majority (85 percent) of those questioned have very small or rather small doubts. Only 15 percent have rather big or very big concerns (Fig. 5).

![Fig. 5: Do you have concerns about the accountability of the voting process?](image)

When asking if they have doubts about the correctness of the voting result and the example of manipulation of votes is given, one quarter of those questioned indicated that they have rather big or very big concerns. The majority, 45 percent, have rather small concerns (Fig. 6).

![Fig. 6: Do you have concerns about the correctness of the voting result?](image)
The issue, where people have the most concerns about is the guarantee of the secrecy of ballot. Thirty percent marked that they have rather big or very big doubts. Seventy percent have very small or rather small doubts (Fig. 7).

![Pie chart showing concerns about the secrecy of the ballot]

Fig. 7: Do you have concerns about the guarantee of the secrecy of the ballot?

Despite of some concerns, the majority of people, 60 percent, indicated to use e-voting if the possibility would exist. Thirty-five percent would perhaps use it and only five percent stated that they would not use it.

Finally, those questioned could optionally give an open statement about e-voting. There was a wide range of answers. Whereas some see it as a comfortable way to give their vote and regret the termination of the pilot project in Thalwil, others stated that every electronic system could be possibly hacked, no improvement can be identified or that they see e-voting as a devaluation of the act of voting.

### 6.2 Conclusion

Generally, the result can be interpreted as a rather high trust in the democracy. The vast majority has few concerns about e-voting. Nevertheless, a fifth of those questioned do have doubts about e-voting and question particularly the correctness of the result and the guarantee of the secrecy of the ballot.
7 Conclusion

When the authors of this paper started to work on this Study Case, the prejudices about e-voting were very little based on the public opinion, on the report of the Swiss Federal Council and the interview with Mr. Langenauer. They all announced the progress and the lessons learned, which were attained during the different phases. Statements sounded very promising, until the interview with Mr. Ragaz was completed. He showed that the security issues should not be left unnoticed and adapted the opinion of the authors.

In the beginning of this paper the following three research questions were mentioned and were answered during this thesis:

- What are characteristics of a secure e-voting system?
- How are the different criteria evaluated at the Swiss e-voting system?
- What are the risks regarding e-voting?

In case of a definitive implementation of an e-voting system it has to be secure without vulnerabilities. The characteristics defined for a secure e-voting systems are the following: Accuracy, Democracy, Privacy, Verifiability and Fairness (Haenzi; Dubuis, 2008). These criteria are used because they include the principles governing the law of elections, which are of prime importance for implementing an e-voting system.

The evaluation of the two interviews with the experts gave very opposite opinions and showed the different perspectives, which are dominating the public. Both of the interviewee agree about the existence of risks concerning e-voting, but they disagree about the magnitude. Whereas Mr. Langenauer argued that the security requirements are almost fulfilled, due to the implementation of the verifiability, Mr. Ragaz has big doubts about the e-voting system. It is questionable if the verifiability can solve every problem regarding security concerns.

One of the main security issues is a server attack. The possibility to attack a server of a canton generate big dimension of control, which could be exploited by resentful people. After a few “CD-issues” in banks, where longstanding employees blow their employers while giving information outside, an insider attack is not preventable. Such an impact would be huge. A further problem is the insecure user platform.
The supporter of the e-voting system mention frequently the argument that it works like the online banking. This comparison is not quite correct. First, the online banking concerns only individual persons, while e-voting involves an entire population. Second and the most important argument is the fact that if something happens no one would probably recognize it. If something occurs in the online banking, it will be detected on the account balance. Furthermore, the secrecy of the ballot, which is firmly established in our legal system, makes it hard to implement a secure e-voting system.

The results of the survey show that the majority of people have small concerns about e-voting, this can be interpreted as a rather high trust in democracy. But surprisingly is the divided opinion of people. The results show that independent of the age and of the web-experience, there are still doubts, particularly about the correctness of the result and the guarantee of the secrecy of the ballot. Furthermore, the evaluation of the survey showed, that people who had experience with e-voting have bigger concerns about the system.

After careful research for this paper, the authors have doubts if the effort for implementing such a system is justified. The e-voting system brings several advantages such as mobility, simplification for visually impaired voters and Swiss expats. But as long as there are still problems and risks available, as long is the system not ready for the implementation. And it is highly questionable if in the next years solutions can be found to face all the risks.

Moreover, the authors argue that nowadays with the postal vote a secure, comfortable, prompt and inexpensive voting system already exists. What attract attention are the extremely high costs of the Swiss confederation: 7.5 Mio. - excluded the expenses of the cantons (Bericht des Bundesrates, 2013, p.95). The question is if that amount is justified and if the expenses should be invested in another e-government project with a higher benefit.

Voting is a sensitive subject and if a mistake happens the impact on our direct democratic system would be enormous and the associated “loss of trust” of citizens would be non-curable.
8 References

Baumgartner, F., 2013: Bald ein Schwarzmarkt für Wahlergebnisse?; Neue Zürcher Zeitung, November 20, 2013: available at:
http://www.nzz.ch/aktuell/zuerich/uebersicht/bald-ein-schwarzmarkt-fuer-wahlergebnisse-1.18187786


Fujiooka, T. Okamoto, and K. Ohta, 1993: A Practical Secret Voting Scheme for Large Scale Elections; Advances in Cryptology - AUSCRYPT '92.


Kanton Zürich, Direktion der Justiz und des Innern, Statistisches Amt, 2013: available at:


Appendix

Questionnaire for E-Voting

Accuracy
Scaled questions:
Does the system guarantee...
  a) ...that the casted votes cannot be altered or replaced?
      □ Not fulfilled  □ slightly fulfilled  □ partly fulfilled  □ fulfilled  □ I don't know
  b) ...that all valid votes are counted?
      □ Not fulfilled  □ slightly fulfilled  □ partly fulfilled  □ fulfilled  □ I don't know
  c) ...that invalid votes are not counted?
      □ Not fulfilled  □ slightly fulfilled  □ partly fulfilled  □ fulfilled  □ I don't know

Open Questions:
  1) How is this criteria technically ensured?

  2) Are there any changes in future (e.g. legal changes)?

  3) What kind of risks can you imagine if the accuracy is in question?

  4) How high is the probability? What is the prevailing impact? (low, medium, high)

Democracy
Scaled questions:
Does the system guarantee...
  a) ...that the eligibility is proved?
      □ Not fulfilled  □ slightly fulfilled  □ partly fulfilled  □ fulfilled  □ I don't know
  b) ...that authorized voters can only vote once?
      □ Not fulfilled  □ slightly fulfilled  □ partly fulfilled  □ fulfilled  □ I don't know

Open Questions:
  1) How is this criteria technically ensured?

  2) Are there any changes in future (e.g. legal changes)?

  3) What kind of risks can you imagine if the democracy is in question?

  4) How high is the probability? What is the prevailing impact? (low, medium, high)
Privacy
Scaled questions:
Does the system guarantee...
a) ...that casted votes cannot be linked to its voters?
   □ Not fulfilled □ slightly fulfilled □ partly fulfilled □ fulfilled □ I don’t know
b) ...that no detection of citizens who voted/did not vote is possible?
   □ Not fulfilled □ slightly fulfilled □ partly fulfilled □ fulfilled □ I don’t know
c) ...that voters cannot prove that they voted in a particular way?
   □ Not fulfilled □ slightly fulfilled □ partly fulfilled □ fulfilled □ I don’t know

Open Questions:
1) How is this criteria technically ensured?
2) Are there any changes in future (e.g. legal changes)?
3) What kind of risks can you imagine if the privacy is in question?
4) How high is the probability? What is the prevailing impact? (low, medium, high)

Verifiability
Scaled questions:
a) Is the individual verifiability given? (voters can verify that their vote is casted as intended, recorded as a cast and is counted as recorded)
   □ Not fulfilled □ slightly fulfilled □ partly fulfilled □ fulfilled □ I don’t know
b) Is the universal verifiability given? (voters can verify independently that all valid votes are counted correctly)
   □ Not fulfilled □ slightly fulfilled □ partly fulfilled □ fulfilled □ I don’t know

Open Questions:
1) How is this criteria technically ensured?
2) Are there any changes in future (e.g. legal changes)?
3) What kind of risks can you imagine if the verifiability is in question?
4) How high is the probability? What is the prevailing impact? (low, medium, high)
**Fairness**

**Scaled questions:**

Does the system guarantee...

a) ...that no early results are available during the voting process?
   - [ ] Not fulfilled   [ ] slightly fulfilled   [ ] partly fulfilled   [ ] fulfilled   [ ] I don't know

b) ...that no early results are available after the voting process?
   - [ ] Not fulfilled   [ ] slightly fulfilled   [ ] partly fulfilled   [ ] fulfilled   [ ] I don't know

**Open Questions:**

1) How is this criteria technically ensured?

2) Are there any changes in future (e.g. legal changes)?

3) What kind of risks can you imagine if the fairness is in question?

4) How high is the probability? What is the prevailing impact? (low, medium, high)
## Umfrage e-Voting

1. Wie alt sind Sie?  
   - □ 18-25  □ 26-35  □ 36-45  □ 46-55  □ 56-65  □ 65+

2. Sind Sie...?  
   - □ männlich  □ weiblich

3. Sind Sie in der Schweiz stimmberechtigt?  
   - □ Ja  □ Nein

4. Haben Sie schon elektronisch abgestimmt?  
   - □ Ja  □ Nein

5. Tätigen Sie ihre Zahlungen per e-Banking?  
   - □ Ja  □ Nein

6. Haben Sie schon einmal online eingekauft?  
   - □ Ja  □ Nein

7. Haben Sie bei e-Voting Sicherheitsbedenken?  
   - □ sehr kleine  □ ziemlich kleine  □ ziemlich grosse  □ sehr grosse  □ ich weiss nicht

   - □ sehr kleine  □ ziemlich kleine  □ ziemlich grosse  □ sehr grosse  □ ich weiss nicht

9. Haben Sie Bedenken bezüglich der Wahrung des Stimmgeheimnisses?  
   - □ sehr kleine  □ ziemlich kleine  □ ziemlich grosse  □ sehr grosse  □ ich weiss nicht

10. Haben Sie Bedenken bezüglich der Wahlfreiheit? (z. B. Korruption oder Erpressung)  
    - □ sehr kleine  □ ziemlich kleine  □ ziemlich grosse  □ sehr grosse  □ ich weiss nicht

11. Haben Sie Bedenken bezüglich der Nachvollziehbarkeit der Wahl? (z. B. Wahlvorgang ist nicht mehr für jedermann verständlich)  
    - □ sehr kleine  □ ziemlich kleine  □ ziemlich grosse  □ sehr grosse  □ ich weiss nicht

12. Würden sie, falls die Möglichkeit bestehen würde, elektronisch abstimmen?  
    - □ Ja  □ Nein  □ Vielleicht
13. Offene Kommentare:
## Resultate E-Voting

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>14</td>
<td>6</td>
<td>20</td>
<td>6</td>
<td>10</td>
<td>10</td>
<td>18</td>
<td>2</td>
<td>17</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

1
<table>
<thead>
<tr>
<th>Teilnehmer</th>
<th>Haben Sie Bedenken bezüglich der Korrektheit des Wahlresultates?</th>
<th>Sehr klein</th>
<th>Ziemlich klein</th>
<th>Sehr groß</th>
<th>Haben Sie Bedenken bezüglich der Wahrung des Stimmengleichheitsrechts?</th>
<th>Sehr klein</th>
<th>Ziemlich klein</th>
<th>Sehr groß</th>
<th>Ich wisse nicht</th>
<th>Haben Sie Bedenken bezüglich der Wahlfreiheit?</th>
<th>Sehr klein</th>
<th>Ziemlich klein</th>
<th>Sehr groß</th>
<th>Ich wisse nicht</th>
<th>Haben Sie Bedenken bezüglich der Nachvollziehbarkeit der Wahl?</th>
<th>Sehr klein</th>
<th>Ziemlich klein</th>
<th>Sehr groß</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Ja</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Nein</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
### Ergebnisse der Umfrage

<table>
<thead>
<tr>
<th>Teilnehmer</th>
<th>Ja</th>
<th>Nein</th>
<th>Vielleicht</th>
<th>Offene Kommentare</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>Der &quot;AKT&quot; der Stimmabgabe wird irgendwie entwertet.</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Jedes elektronische System kann geknackt werden, siehe ZV NSA. Daher bevorzuge ich die briefliche Stimmabgabe.*

*Die Zukunft des E-Voting liegt - wie bei allen anderen Kommunikationsbereichen - in der elektronischen Welt. Relevant für deren Erfolg ist eine praktische, einfache und aufnahme Benutzeroberfläche.*

*Ich begrüße die Beendigung der E-Voting Möglichkeit in der Gemeinde Thalwil.*
Statement of Authorship

We hereby declare that we have written this thesis without any help from others and without the use of documents and aids other than those stated above.

We have mentioned all used sources and cited them correctly according to established academic citation rules. We acknowledge that otherwise the department has, according to a decision of the Faculty Council of November 11, 2004, the right to withdraw the title that we were conferred based on this thesis.

Fribourg, December 1, 2013

Andrea Baumann

Daniela Häberli