Transparency & eVoting in Switzerland

December 2, 2012

Pierre Vanhulst  Mathias Seuret
pierre.vanhulst@unifr.ch  mathias.seuret@unifr.ch

Work done for the seminar “Electronig Government” given at the University of Fribourg (Switzerland) by Prof. Dr. Andreas Meier
Assistant : Luis Teran

Abstract
As a way to ensure democracy, in several parts of Switzerland, people have the right to assist physically to the counting of the ballots. Moreover, citizen are usually randomly chosen for counting. This whole process is as transparent as possible and very easy to understand and to check. The new eVoting system which has been tested for a few years grants us with a better comfort and may allow more people to vote, but poses new challenges to guarantee the transparency which is so important to any real democracy. This small study focuses on the transparency of the eVoting system of the canton of Geneva.

Keywords : eVoting, transparency, privacy, eGovernment, eDemocracy
### Contents

1. **Introduction** 3
2. **Objectives of this research** 3
3. **Definition and aims of eVoting** 3
4. **Transparency and privacy** 4
   - 4.1 Relevance of transparency and privacy 4
   - 4.1.1 The survey 4
   - 4.1.2 Results 6
5. **Voting systems in Switzerland** 10
   - 5.1 Non-electronic voting system 10
   - 5.2 Postal voting 11
   - 5.3 eVoting 11
     - 5.3.1 Overview of current eVoting systems in Switzerland 12
     - 5.3.2 Transparency and privacy in eVoting 13
6. **The eVoting system of Geneva** 13
   - 6.1 How it works 13
   - 6.2 Transparency 15
7. **eVoting in Belgium** 17
   - 7.1 BeVoting - a Belgian study about electronical voting 18
   - 7.2 Current State of eVoting in Belgium 18
8. **Interviews** 18
   - 8.1 Reto Koenig 18
   - 8.2 Ulrich Ultes-Nitsche 19
   - 8.3 Alexis Roussel : opinion of the Swiss Pirate Party 19
     - 8.3.1 Issues with eVoting 20
     - 8.3.2 Benefits 20
     - 8.3.3 Possible Improvements 21
9. **Conclusion** 21
   - 9.1 Personnal conclusion of Mathias Seuret 21
   - 9.2 Personnal conclusion of Pierre Vanhalst 22
10. **Acknowledgments** 22
11. **Annexes** 25
1 Introduction

Switzerland might be the country where people vote the most often. Several times every year, hundred of thousands of citizen go to the polls and give their opinion. Postal vote has been possible since 1992, these ballots being inserted into the urns when the polls are closed. Eleven years later, in 2003, some citizen of the canton of Geneva voted through Internet for the first time. In 2012, citizen from twelve cantons did so.

The transparency of the election is necessary for a democracy. All citizen must be allowed to understand the system and to verify it. In the current non-electronic voting system, people write their choices on pieces of paper, and puts them into an urn. This system is simple but efficient; all citizen understand how it works and some of them are randomly chosen to supervise the polls and count the ballots. Also, all citizen are allowed to oversee the counting of the ballots in order to verify that everything is done correctly.

Do the eVoting systems used in Switzerland since 2003 still guarantee the same level of transparency? This is the main issue addressed by this paper.

2 Objectives of this research

We intend to find out what is the current state of transparency in the current eVoting system in Switzerland. Because we cannot just ask How much transparent is it?, we will have to learn how it works try to get details of its inner-working and ask questions to people involved in it.

We decided to mainly focus on the Geneva eVoting system because it was recently involved in a session of tests which ended up with challenged results. Moreover, people who manage it speak French and the documentation is also available in French. Another reason for focusing on the Geneva system is that we wanted to check the transparency for a lambda citizen who wants to know how the system works, not the transparency for students who are doing some research on the topic. A family member of one of the authors of this document, who lives in Geneva, agreed to let his name being used in order to contact the eVoting staff, with the condition that he receives a copy of the report when it is done.

In order to be as unbiased as possible, we also decided to interview persons from both sides: some who are supposed to be against eVoting and some others who are supposed to be proponent.

3 Definition and aims of eVoting

"Electronic voting (also known as e-voting) is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes.” [1]

According to most definitions, e-Voting is a very wide term regrouping different electronical means to vote. Those range from terminals that make counting easier to accessibility devices allowing disabled people to vote. This paper will mainly focus on the e-Voting as a way to vote from home through a regular web browser, more specifically in Switzerland.
According to Roussel, the main purpose of eVoting in Switzerland is to increase the voter turnout, by improving the comfort of the citizen. Comfort should mostly benefit Swiss citizen living in foreign countries, as well as workers unable to vote before polls are closed and citizen who were generally discouraged by the traditional, heavy voting procedure.

4 Transparency and privacy

Transparency is tightly linked to privacy. Any eVoting system has to guarantee both: the vote of any citizen must be kept secret, but the whole process of counting votes must be transparent so that everybody can trust the results.

If the voting system lacks transparency, then it may not be possible to know if somebody has modified the results, either by not counting correctly, or by creating fake votes. With a non-transparent system, citizen have to trust the few people who manage the poll offices and count the votes - which does not suit a democratic system.

4.1 Relevance of transparency and privacy

At this point, one question might arise: why are privacy and transparency so relevant to a democratic system? An assumption was made that many people usually break their own anonymity by communicating about their political opinion on social networks. Is privacy still so important while citizen agree to reveal their voting intentions? Is it the same for transparency? Is the attachment to those values still strong?

4.1.1 The survey

These fundamental questions were first answered by submitting a survey to a hopefully very large group of people (from young adults to seniors, males and females, Swiss and foreigners). The survey was designed online, but a printed version was also used in order to reach groups of people refractory to Internet. As we wanted opinions and not facts, we decided to use qualitative questions rather than quantitative questions in order to let people evaluate themselves relatively to their own scale.

Following are the final questions asked in our survey. A first version was submitted for review and modified accordingly. The original form[2], which is in French, contains the following questions:

- On a scale of 1 to 6, how important is secrecy of the vote to you?

- How often do you speak of your voting intentions online (blog, social networks, ...)?
  - Never
  - Sometimes
  - Always

- Do you think your privacy is guaranteed when you vote online?
  - No
• Would you agree to vote online, if this implied risk for your privacy?
  o No
  o Yes
• Did you know that Swiss citizen have the right to check if the votation system is working correctly (by assisting, among other things, to the counting of the votes)?
  o No
  o Yes
  o I thought so
• On a scale of 1 to 6, how important is this right to you?
• Is it legitimate that every citizen who asks for it can access a copy of the softwares used by the e-voting system for testing purpose?
  o No
  o Yes
  o I don’t know
• Would you agree to vote online, if this implied that you couldnt check if the votation is working correctly?
  o No
  o Yes
• To which age group do you belong?
  o 18-25
  o 26-35
  o 36-45
  o 46-60
  o 61+
• Are you...
  o Male
  o Female
• Do you have the right to vote in Switzerland?
  o No
  o Yes
• What is your main mean to access Internet?
  o Computer
  o Tablet
  o Smartphone
• On a scale of 1 to 6, how often do you use Internet?
4.1.2 Results

Our final sample size was of 10 persons. While this might imply poor results in most usual cases, the homogeneous answers of our population made it very likely that the final results of a larger population wouldn’t be very different.

![Figure 1: The importance of secrecy](image)

The first question clearly indicated that our population cared about secrecy of the vote. The result is visible in figure 1: 60% give an importance of 6/6, and 40% of 5/6. This should be enough to propel privacy to the head of concerns to be taken into account when designing a voting system (regardless of the technology).

![Figure 2: How often people speak online of their voting intentions](image)
Without surprise, a generational gap was found in the second question as younger people tend to be more prolix online than older people. In figure 2, we can see that 50% people never speak of their voting intentions online, but 40% always do so.

**Figure 3: Trust in eVoting privacy**

The majority of the interviewed people (60%) do not know if eVoting preserves the privacy (cf. figure 3.

**Figure 4: Would people agree for a system without privacy ?**

This question being closely related to the first one, the result seen in figure 4 is in the keeping.
As seen in figure 5, a majority of the population believed that there was something in the Swiss law that could guarantee transparency of the system, though most of this majority didn’t seem to know exactly what. Still, a significant part wasn’t aware of that right.

We assume that this right for transparency seemed less important than privacy for our population, as some of surveyed people didn’t exactly know what to do with it (cf. figure 6) and believed that making sure that the votation isn’t going wrong is the duty of the government, and not the right of a citizen.

This question raised a minority of no, as seen in figure 7, which were likely answered because of the idea that a information system could be more easily compromised if its source code is known.

As expected, the answers seen in figure 8 are globally in-line with the previ-
The answers we gathered clearly expressed how much surveyed people cared about their civic rights and aren’t ready to give them up consciously. Our attempt to confront their use of Internet and their civic consciousness had little success.

Regarding privacy, further discussions and remarks from our population suggested that though some revealed their voting intentions on certain occasions, they still felt like they had the control over this - thus our assumption that those who talk about voting intention online are more likely to sacrifice the secrecy of their vote was irrelevant.

More importantly, some pointed out that keeping the final vote secret is the best way to ensure that no pressure can be exerted on citizen. This is why secrecy of the vote is one of the pillars of democracy, as it prevents people from checking what others really voted.

While most of our population didn’t exactly know about their right to ensure that the system is working correctly, they were pretty much attached to it as well. Some, though, believed that accessing the source code wasn’t relevant as it
takes a lot of time to study even for a professional. Others raised that knowing the source code might be a risk for the system: in their opinion, if the software is easy to know, it could mean that it is easy to hack.

5 Voting systems in Switzerland

The following sections will discuss the way that voting systems work in Switzerland and how they could achieve both transparency and privacy. Those explanations will put in perspective issues related to the e-voting system analyzed later in this paper and provide bases for reflection about possible improvements.

5.1 Non-electronic voting system

The non-electronic voting system of Switzerland has been working without important issues for a very long time. It can ensure both transparency and privacy. The steps for voting on paper are the following ones:

- Every citizen gets by mail a paper which authorize them to vote and the voting paper(s).
- They fill the paper and go to the poll of their town. There, they show the authorisation to vote, and then:
  - They put the authorisation to vote in an urn.
  - They have a stamp put on the voting paper, which is folded so that its text is not visible. The stamp must be in the middle of the paper, not in a specific location. In that way, it is not possible to know the vote of a specific citizen by putting the stamp in a special place for that person only.
  - They put the voting paper in a second urn.

Nobody in the poll ever manipulate at the same time both the voting authorisation and the voting paper. Nor does anybody even touches them before they are taken out of the urns. When the urns are opened, their content is immediately tossed so that nobody can know in which order the papers were inserted in them. This guarantees a good level of privacy and to our best knowledge there has never been large scale problems with it.

The system is also designed in a way which allows much transparency. Citizen are randomly chosen to manage the poll offices. The whole process is also simple enough for everybody to fully understand it, and all citizen are allowed to watch the counting of the ballots.

With this system, it is possible for each citizen

- to be sure that their vote is in the urn,
- to be sure that nobody knows their vote,
- and to check if the votes are counted properly.

Moreover, no fake votes can be inserted into the urns because then the number of authorisations would not correspond to the number of vote papers.
5.2 Postal voting

In Switzerland, postal voting has been possible since 1992 and is much used today. It has two main advantages:

- Citizen living outside of the country can vote without having to travel to Switzerland.
- Citizen who cannot go to the poll offices when they are open (e.g. people who are working on weekends) can vote too.

In order to vote in that way, the citizen receive with the vote papers two envelopes. A large one and a smaller one. They have to put the vote papers in the small envelop, and the voting authorisation with the small envelop in the large envelop. They then mail it to the poll office of their town, or put it directly into the mail box of the poll office.

These postal votes are processed by the citizen counting the usual votes. The procedure is quite simple:

- They open the large envelop.
- They check if there is a valid authorisation with the small envelop.
  - If there is none, they destroy it.
  - If there is one, they put it into the urn along with the authorisation given by people who came at the poll office, and they put the small envelops into another urn.
- When all large envelops have been opened, the small envelops are tossed and opened. The voting papers they contain are then put into the urn containing the papers given by the people who came at the poll office.

After this, any postal vote is processed in the exact same way as standard votes. This process is almost totally transparent. There is a slight uncertainty on what happens in the envelop while it is being transferred to the poll office, but otherwise it is manipulated only by randomly chosen citizen.

There is a small privacy issue in the poll office: somebody could potentially open the small envelop directly after having checked the voting authorisation which contains the name of the citizen. However, doing so in the poll office without being noticed by other people would be difficult.

5.3 eVoting

Electronic systems belong in two main categories:

- Electronic machines placed in poll offices (people have to go there to use the device),
- Voting application using an Internet connection to vote on a remote server from any place, at any time.
In Switzerland, eVoting systems adopt the second option. People can vote from home using authorizations received with the vote envelop.

If eVoting offers more comfort, it should still provide the same level of transparency and privacy as the legacy voting system in Switzerland. There is clearly a transparency issue which is difficult to solve: most citizen do not know much about computers, security and cryptography. Most of them do not have the skills required to verify that everything is done correctly: that the votes are correctly received, saved and counted, and that the privacy is conserved during the whole process.

Conceiving an eVoting system which guarantees both privacy and transparency is a very difficult challenge.

5.3.1 Overview of current eVoting systems in Switzerland

Several cantons have their eVoting system.

Neuchtel uses an eGovernment system called Guichet unique. This system centralizes different administrative tasks, such as enforcement office or voting. A Java applet in a web browser is used for eVoting.

Zrich has used an eVoting system developed by (and belonging to) a private enterprise. Amongst all its features, it notably allowed to vote by mobile phones through SMS. In November 2011, the canton has decided to stop using eVoting until they are able to offer this option to the whole population. Cantons using the system of Zrich (Fribourg, Solothurn, St. Galle, Grisons, Argovie and Turgovie) intend to continue using this system despite of it[3].

Geneva has developed its own eVoting system. It is used by the cantons of Bern, Luzern and Basel Stadt. We focused our study mainly on this system.

The federal law has several articles concerning the electronic votes. Some specifications are mandatory. If the eVoting system may derogate to the law about postal vote and vote in the poll offices[4], a canton which wants to use this system must still get the authorization of the Federal Council[4]. If the canton which experiments eVoting decides how to define if a ballot is valid or not[5], it is probably because the implementation of eVoting is not the same in all cantons.

The privacy is pretty well protected by the law. It states that nobody must be able to break the privacy of the vote[6]. It must not be possible to identify an elector at any time; not during the transmission, while marking in the database that the elector has voted, nor with the content of the electronic urn[7]. The data used to verify that no user votes more than once must not either be usable to establish the identity of the voter[7]. The order of the votes in the urn must not be usable to know the order in which they arrived into the urn[8]. No information necessary during the electronic processing must be usable to break the privacy[9].

Some articles also indicate that the system must resist to fraud. It is clearly stated that systematic fraud must be impossible[6]. Security measure must prevent all possibilities of systematic fraud[6]. The system must also make sure that no message can be displayed in the foreground of the screen while the elector is using the voting device[10]. All users must also receive proofs of the authenticity of the website they use for voting[10]. During the voting session, the involved servers must not be used for any other task[8]. And finally representatives of the electors must be able to watch the counting of the electronic votes[11].
5.3.2 Transparency and privacy in eVoting

Because of its complexity, eVoting is more difficult to understand than traditional systems. It is clear that most citizen would be able to understand only a part of it. Moreover, they cannot watch the data being processed. The system is centralized and managed by a small number of people. A question arises: how can such a system be transparent?

Different parts of the eVoting system can have different transparency levels. For the system to be fully transparent, we think the following conditions should be fulfilled:

- Detailed information about how the system works should be available for all citizen.
- All citizen should be allowed to study and test the source code of all softwares involved in the eVoting system.
- All citizen should be able to check if the softwares running on the servers are the correct ones.
- The system should be designed in such a way that it could be possible to prove that
  - All sent votes are correctly received,
  - all correctly received votes are correctly saved,
  - all correctly saved votes are correctly counted,
  - and no saved vote is fake.
- Data must be stored in a way which guarantees privacy during all steps of the procedure, and all citizen should be granted access to it at any time after the voting is over.
- All modifications of the stored data are logged, and all citizen are allowed to consult these logs.

Most citizen would not be able to study and verify an eVoting system: only experts can do so. But it should not be used an excuse for limiting the transparency of these systems. If not all citizen know much about security and cryptography, there are many experts among them.

But these conditions would be very difficult to fulfill and it could bring some problems. For example, the access to the source code could be used in order to attack the system. It could be done by citizen, which would already be bad, but it could also be done by other countries, which would be worst.

6 The eVoting system of Geneva

6.1 How it works

The system used by Geneva was first developed by a private company for commercial purpose. Since then, the State took control of it and team of developers is constantly looking for improvement, both on the security and the transparency side.
An explanatory website - “A coeur ouvert”[12] (literally : “Open Heart”) - has been created to educate citizen about the way Geneva’s system work. It describes quite precisely how the system is working, in four steps. Here is a short summary :

- **Initialization**: sending the preparatory data to the server, including identification data, information about the votation, ...

- **Sealing of the ballot box**: using asymmetric keys, the ballot box is sealed so that nothing can touch it unexpectedly. Seven officials are required for this step, diminishing the risk of corruption. “A coeur ouvert” offers some rather easy-to-understand explanations about how the asymmetric key algorithm and process work.

- **Voting session**: the voters connect to the website with the browser, using a protected connection. They must first login by giving their date of birth and town of birth and a password. Only the hash of the password is known by the server. Then, in order to prove that the vote was correctly received by the real server, a confirmation code, which is visible on the voting papers, is sent back to the voter.

- **Counting of the ballot box**: there again, the number of participants is clearly indicated. Each of these participants have a specific role to attend: they cannot do anything alone but are required to count the final result. Quantum physics is used to randomize the order in which votes are retrieved, in order to simulate legacy votations mixing of votes.

At this stage, it is hard to figure if the system poses any risk for privacy. On the other hand, the question of transparency is more relevant. It should be mentioned that all this process takes place in one single environment, by opposition of legacy votation that decentralizes data over several polling stations.
6.2 Transparency

In order to know how transparent the eVoting system of Geneva is, we decided to contact the help desk with some questions without stating that our interest was academical. We used the identity of a family member of one of the authors of this document, who gave his agreement for this, with the condition that he will receive a copy of this document. In the e-mails we sent, we avoid using technical vocabulary.

We first asked them the following questions:

1. How can you guarantee that one person can vote only once?
2. How can you guarantee the privacy?
3. As citizen of Geneva, are we allowed to see the source code of the different programs?
4. Have you had problems during the previous eVoting sessions?
5. If there is a problem, are you able to solve it without breaking the privacy?

At this time, we were mainly interested by questions 3 and 4. Giving access to the source code is important for transparency. We also knew that there had been a problem in Lucerne, where the eVoting system of Geneva is used: somebody was able to vote twice and their second vote has had to be erased [reference]. We also learned that at least once when the electronic urn was opened, the program failed and did not display anything. Although several persons were watching the screen in order to make sure that everything worked correctly, no one had noticed the failure and some were surprised when the technician said he had to restart the procedure\(^1\). We wanted to know if they would admit these problems or try to hide them.

We received a brief and anonymous\(^2\) answer indicating that we can get more information about eVoting on a document available on the website of Geneva[12]. We were not much satisfied by this answer.

We then sent a second mail, asking more questions, still with a non-technical vocabulary:

1. If some malicious software modifies what is displayed on the screen of a user and changes their vote, can you detect it?\(^3\)
2. One of your main security is that nobody excepted the states knows from where the citizen were born and their birth date. I have written this on Facebook, so if somebody steals my voting envelop, can they vote for me?
3. If somebody tries to send fake votes, for example after having stolen an envelop, can you find out who it was?
4. You write in the documentation that citizen who are interested can get a copy of the source code, who should I contact if I want to read it?

---

\(^1\)This information was given by Alexis Roussel, who was present in the room.

\(^2\)From “Evoing-support-tech-n2 (DU)”

\(^3\)The system must prevent it[10]
5. During previous eVoting sessions, have you had any problem? For example pirates trying to send fake votes, or people who did not have the correct key?

6. Which security software do you use on the eVoting server in order to make sure it doesn’t get infected by malicious software?

The second answer arrived three days later, and was as anonymous as the first one. After thanking us for being interested in the electronic voting solution of Geneva, they said that the help desk team is not authorized to answer to questions about the detailed working of the electronic voting solution. They said we should contact M. Michel Chevallier, who is working at the State Chancellery.

We then forwarded the e-mail to M. Chevallier and he replied that he could not address all our questions, but he would ask for information to his colleagues who look after the technical parts of the eVoting system. Then, he answered to some of our questions:

- “One of your main security is that nobody excepted the states knows from where the citizen were born and their birth date. I have written this on Facebook, so if somebody steals my voting envelop, can they vote for me?”
  Most people do not know the town in which they were born: they have had to put a picture of an identity card in the FAQ to show where this information can be found. So he thinks that most people will not write this information on Facebook. He also indicated that Facebook did not exist when the eVoting system was designed, and that the double-safety of asking both the date of birth and the town of origin is the safest protection against identity theft in the eVoting system. Later, they intend to use electronic identity cards, but such cards are not yet used in Switzerland.

- “You write in the documentation that citizen who are interested can get a copy of the source code, who should I contact if I want to read it?”
  The source code can only be consulted in their office, they do not send it. The article 60, paragraph 10, of the law on political rights indicates that the source code can be tried (prouv in French) by every voter who justifies a scientific or ideal interest, and who agrees to to keep it confidential. They must contact the State Council and give a motivation and may or may not be granted access to the source code.

- “During previous eVoting sessions, have you had any problem? For example pirates trying to send fake votes, or people who did not have the correct key?”
  In February 2012, a citizen of Lucerne (a canton which uses the eVoting system of Geneva) was able to vote twice, without bad intent, because of a wrong setting of the database⁴. He thinks some people may have had problems to use the eVoting system because there may exist 50 to 60 different computer configurations and they cannot make a system compatible with all of them because of security and encryption requirements.

⁴We have learned that the vote was not atomic, and that this problem is now solved.
“Which security software do you use on the eVoting server in order to make sure it doesn’t get infected by malicious software?”

He does not know which antivirus is used on the servers of the canton of Geneva. For the eVoting they use another defence: there is a limited number of valid ballots, and any invalid ballot is discarded. A ballot containing a virus would not be considered as valid, so it would not be inserted into the urn.

Two weeks after this first answer, we did not receive the more technical information he said he would send us. We did not recontact him to ask for them again.

We can understand the first answer of the help desk: most people who contact a help desk did not read the documentation first. Some of our naive questions used to hide the fact we have some knowledge in informatics had indeed an answer in the documentation, so in our second mail we indicated that some questions had so far not been answered.

Their second answer shows a problematic issue: the help desk is not authorized to give information about how the system works. If we want to ask questions, we have to send them to a single person. It may limit the responsiveness if many people want to know more about eVoting, but this is not a critical problem because technical questions do not have the same priority as questions about how to use the system during an eVoting session. But this person cannot answer to technical questions either and has to transfer them to other people.

The lack of efficiency is not a problem either, but the lack of answers to technical questions which we met is an obstacle to transparency.

We can also make a little parenthesis about security. We do not know if the current eVoting system of Geneva is safe even if the computers of the voters are infected by malicious software because this question was not answered. Nothing in the documentation is said about this, and we can expect that if such a security existed, it would be stated somewhere. The way to verify the identity of voters by asking the town of origin and the date of birth does not seem to us as secure as claimed, but it seems at least as much secure as the signature which must be written on the voting authorization in case of postal vote.

7 eVoting in Belgium

While Switzerland is slowly adopting eVoting, other countries already went through this electronical revolution. Observing how this process worked and what were its consequences might give us insights about how to improve the Swiss systems. Amongst the different considered countries, Belgium proved to have a very complete, advanced and accessible source of information.

Belgium was one of the first countries to adopt electronic voting, as it has been used since 1991. It is important to note that vote is mandatory in Belgium. Thus the purpose of eVoting isn’t about increasing the voter turnout but rather to make the counting easier. When speaking of evoting in Belgium, people mostly think of terminals. Those were used to make the counting easier and debates about how costly they are still stir Belgium. Still, other solutions were also considered.
7.1 BeVoting - a Belgian study about electronical voting

In 2007, Belgium government asked a Consortium of Belgian Universities a large study about eVoting in general, including comparison with other countries and perspectives for all the different eVoting means and technologies. This massive study provides tremendously precious information about the state of eVoting in the world.

The first part of the study focuses on eVoting state, both in Belgium and in the world. Switzerland is described in general terms. Oddly, the study quotes two Swiss sources stating different things about the increase of voter turnout: one says that it increased by 20% in Geneva thanks to eVoting while the other that this increase isn’t significant[13].

The second part of the study considers different uses of eVoting. Amongst those uses, Remote/Internet voting based on homomorphic encryption directly refers to the system discussed in this paper. Before explaining how the system works, the study clarifies that the Consortium doesn’t recommend this solution: while they believe it is possible to create a system that would ensure privacy, its lack of maturity and its complexity will not inspire confidence to the citizen - something that is required for adoption. Amongst the technical issues, the fact that voters terminals cannot be secured before voting is one of the main stumbling block of the system.

7.2 Current State of eVoting in Belgium

Following the recommendations of the study, the government has planned to use a new system of eVoting developed by private companies and specifically customized for Belgium. This system is a improved paper-based voting and no plans are made for an Internet voting system for now. Elections occured mid-october and feedbacks about electronic voting are still very scarce.

Sources: [14] [15] [16] [17]

8 Interviews

We interviewed several persons involved in eVoting. We decided to contact people who were presumably for and against eVoting in Switzerland, in order to have the point of view of both sides.

We will present the outcome of these discussions sorted by alphabetical order of the family names.

8.1 Reto Koenig

Reto Koenig is a professor of informatics in the Berner Fachhochschule. He is also a member of the E-Voting-Kompetenzzentrum Schweiz association. We had a discussion with him about the transparency and privacy issues in eVoting.

He does not believe that allowing people to look at the source code is the most important point for having a transparent system. Sharing information about the inner working of the system with enough details to prove mathematically that it satisfies the correctness of the results and the privacy, and allowing people to do the proofs themselves is necessary.
A major difficulty to make a system which respects both transparency and privacy is that people must be able to check themselves if their vote has been counted correctly. But if it is possible for citizen to ask to the system what they voted, then other people could threaten them, tell them what to vote and then verify if they voted correctly. This would be very dangerous for democracy.

Another problem is that people should be able to verify that all votes stored in the electronic urn are valid votes, and that all valid votes are stored into the urn. Data should only be appended to the database, no vote, even invalid ones, should be erased.

The transparency of the eVoting system of Geneva could be much improved. Cryptography provides methods to do so, but when the system was designed, they were not taken into account.

He has been talking with the persons involved in the eVoting system of Geneva for a long time. One of the main problems he met was that legal experts are not cryptography or security experts; they have a different vocabulary and did not understand each others. Another problem is that security issues which seem important for a scientist in computer science may seem negligible to legal experts, especially if solving them would mean to have to redesign a major part of the system.

8.2 Ulrich Ultes-Nitsche

Dr. Ulrich Ultes-Nitsche is a professor at the University of Fribourg (Switzerland), and the president of the E-Voting-Kompetenzzentrum Schweiz association.

His opinion on eVoting is surprising, especially because he is the president of the association cited above. For him, paper vote is enough, it works best and politicians want eVoting systems because it seems modern and they believe a modern country should have them. Therefore M. Ultes-Nitsche thinks that eVoting must be improved: we cannot avoid it, so we should at least do it well.

The system of Geneva is not verifiable yet and although some security issues have been addressed, some of them still remain. A simple example is denial of service attacks (sending so many requests to the server that it cannot answer to all of them, including the legit ones). So far, excepted by having enough servers that they can process all requests, there is no solution for a service to resist to such an attack.

A major problem of eVoting systems is that the protocols used must be complex to make sure that the results cannot be manipulated, but the more complex a protocol is, the more complex the proof that it works correctly are.

He thinks the current eVoting system of Geneva can be used, but only for minorities, like Swiss electors who do not live in Switzerland, and its flaws should be fixed.

8.3 Alexis Roussel: opinion of the Swiss Pirate Party

One of the most convinced opponent of eVoting in Switzerland is the Swiss Pirate Party. This governmental organization takes digital life at heart and intends to defend Swiss people against potential issues related to information technologies.
The Party was notably wary about Genevas tests in 2012 and responded quickly when the bug was disclosed. Whereas Swiss government spoke of a success - as officials were able to spot the mistake and correct it - the Swiss Pirate Party wondered how this mistake might have happened, how was this mistake spotted, how was it corrected and why wasn’t it possible to access the source code of the program in order to make sure there isn’t any other vulnerability. As the law states that citizen can access the source code under conditions laid down by the Chancery, the Party was eventually granted a glance at the source code late 2012. Unfortunately, by the time this paper is written, experts are still analyzing it and a non-disclosure agreement prevents them from talking about it before the end of the analysis.

Nevertheless, Alexis Roussel, vice-president of the Party, agreed to answer questions regarding the official position of the Party and the incident.

According to M. Roussel, the Swiss Pirate Party is mainly divided into two groups: those who refuse eVoting as they believe it cannot work properly and those who want to make current systems better. The distribution of these groups rely, inter alia, on cantons: in Geneva, people voted to adopt eVoting and the party supporters do not question this decision, implying that they are mostly working towards improving the system rather than dissuading people and politics from using it. Yet the whole Party will try to restrict as much as possible wider adoptions of eVoting systems if they do not provide sufficient guarantees for transparency.

8.3.1 Issues with eVoting

The Swiss Pirate Party believes that paper voting has acquired, after centuries of improvement, a robust methodology preventing the State from abusing its authority. This methodology relies on several points, including decentralized polling stations (which imply that massive corruption would ask for the involvement of many officials) and ease of understanding (the system itself is pretty simple).

As M. Roussel explained, most citizen cannot understand all the details of the eVoting system and thus, they cannot clearly find out when something is going wrong. On the opposite side, when a citizen believes that something went wrong, proving it is almost impossible: M. Roussel spoke of several suspicions of fraud that were brought to court and dismissed as the judge hadn’t anything tangible to take into account. Moreover, in Geneva, data is centralized and it wouldn’t ask for many people to corrupt it and impact the global votation.

8.3.2 Benefits

The benefits of eVoting are also questioned by the Swiss Pirate Party: M. Roussel stated that there was no significant increase of the voter turnout, nor was the eVoting a more comfortable way to vote because it still requires a lot of steps that aren’t intuitive for citizen who aren’t used to information technologies. The Party found out that those who mostly benefited from eVoting were Swiss living in foreign countries (50% of them used eVoting) and citizen voting at the last minute (since they can submit their vote later).
8.3.3 Possible Improvements

M. Roussel proposed several ways to improve the eVoting system. First, there should be new means of control that would allow people to figure when something is wrong, thus increasing transparency. Human controlling (who does what, where and when) works rather well with e-voting systems, since it works the same way as with the traditional voting systems. Yet it is hard for citizen to understand when the software behaves abnormally. As Reto Koenig suggested, adding additional feedbacks that would help citizen to see what is going on would be a good step toward transparency. For instance, comparing results to political forecasting, checking the ballot boxes and some other similar suggestions were made in that direction.

The idea of decentralization was also discussed with M. Roussel. It seemed a good idea as this would limit the risk of massive corruption of the ballots. The eVoting system should strive to work like the legacy system as much as possible.

The Party has also developed its own eVoting system, called Pivote[18]. According to M. Roussel, its transparency is exemplary, though it couldn’t be adopted for a very wide audience because of the way it currently works.

9 Conclusion

This paper has shown how the different Swiss eVoting systems work, mainly regarding transparency and privacy. Neuchtel and Zurich’s systems were briefly exposed and the Genevas system was discussed in details. Before that, a more ethical question was raised about the real need of transparency and privacy, proving that these two values were still most relevant to everyone.

This paper was also intended to confront divergent opinions regarding eVoting, but it happened that specialists usually agree on many points - a proof that conciliation is indeed possible. From those opinions emerged the fact that the most important concern regarding current use of eVoting isn’t privacy, but transparency. Solutions were presented and could currently be applied to allow a better, global understanding of eVoting by the citizen.

9.1 Personnal conclusion of Mathias Seuret

I have so far been chosen twice for working in the poll office and counting the ballots. Working in the poll office in my village is rather nice because most people stop to talk for a few minutes. However, counting the ballots is fastidious, time consuming and nobody seemed to like doing this. Moreover, it is not possible to have conversations while counting because we have to stay focused in order not to do mistakes. When I first started this study, I was thinking that eVoting could save people from doing this unpleasant task. However, as computer scientist, I was feeling a bit uncomfortable with the idea of letting machines manage the democracy of my country.

Then, while learning how the eVoting system of Geneva works, I started to like the idea. Secured encryption in both ways, secret numbers hidden under holograms, and even random number generators based on quantum physics, that really impressed me! Unfortunately, after reading the documentation, when we started to study the privacy and the transparency of the system, I understood that there were
some issues hidden behind a smoke screen. The transparency is not guaranteed, we cannot verify if our votes are really counted. We cannot “see” the inner working of the system, we have to trust people who tell us that everything is all right. Even if I believe that as long as no pirate or other country attacks the eVoting system everything will be fine, I think a great deal of work is still necessary to improve its transparency, which is now much insufficient.

9.2 Personnal conclusion of Pierre Vanhulst

As a Belgian citizen living in a foreign country, it is mandatory for me to vote and this has proved to be a pain because of the heavy, time-consuming procedure. Aware of the problem, the Belgian government deployed a good deal of new voting options and I wasn’t surprised to find that the eVoting was being tested since a long time. This explains why I was quite interested by eVoting at the start of this study. Moreover, User Centered Design is amongst my main field of research and new techniques for improving ease-of-use - no matter the context - raises my interest.

Application of eVoting didn’t prove to be very rigorous so far and it clearly has to be improved before being applied officially. Fortunately, while they aren’t really inspired by this idea, specialists are confident that information systems can be secure enough to allow needing people to use eVoting (citizen living in foreign countries, disabled people, ...). In that respect, a further study in this field could focus on Pivote, the software developed by the Swiss Pirate Party, with the aim of adapting it to a larger group of persons.

While I clearly don’t think that eVoting is a worthy need for regular people, it will clearly make life easier for a significant part of the population. Establishment of a decent system will take some time, though, and this cannot be rushed for irrational reasons such as “call for modernity”.

10 Acknowledgments

We would like to thank Charles Seuret for his involvement in this study, as well as all the anonymous surveyed people who answered our questionnaire. This paper wouldn’t have been possible without the kind participation of Alexis Roussel, Reto Koenig, Ulrich Ultes-Nitsche Michel Chevallier : thank to all three.
References


[2] Google docs [Internet]; 2012 [cited 2012 Dec 02]. Questionnaire sur le vote electronique; [about 1 screens]. Available from: https://docs.google.com/spreadsheet/viewform?formkey=dDhrVS1BZ01qWkFEcloydjdKQkZtQ3c6MQ.


11 Annexes

Demographic information

Figure 10: Age of the participants to the survey

Figure 11: Their sex
Figure 12: Right of vote in Switzerland

- Yes: 80%
- No: 20%

Figure 13: Means of access to Internet

- Computer: 100%
- Smartphone
- Tablet
Figure 14: How often they use Internet