SwissiVi: Proof-of-Concept for a Novel E-voting Platform

Philémon von Bergen

Bern University of Applied Sciences, CH-2501 Biel, Switzerland
vonbp3@bfh.ch

Abstract. Electronic voting is a more and more discussed subject. But there are still unsolved problems, like the secure platform problem. The Bern University of Applied Sciences has developed a concept addressing this problem by introducing two additional components, namely a secure voting device and a voting card. This concept has been implemented as proof-of-concept by two students in their bachelor thesis. This paper gives an overview of the concept, explains the work done in the project and analyzes the obtained results.

1 Introduction

With the evolution of the information society, electronic voting, also called e-voting, becomes more and more a hot subject. This applies especially to Switzerland whose citizens living abroad can vote only through postal voting. Since they receive voting material by post and since mail is not everywhere as reliable as in Switzerland, it happens frequently that the voting material arrives to late. E-voting would be a great alternative which would solve this problem. In a second time, it could also be introduced as an alternative to the two actual voting possibilities, namely ballot box voting and postal voting, for every citizens of Switzerland.

The probably easiest way to do e-voting would probably be a single web platform on which the voter can display the proposals and give an answer to them directly on this web platform. However, with this implementation, there is a still unsolved problem called the *secure platform problem*. It can be described as follow: let's imagine the voter is using a computer infected by a malware. He calls up the voting website and makes his vote. As the malware has, per definition, a total control over the computer, it can know what the user has voted. So we have a loss of confidentiality. That's our first problem. The second problem is that the malware could also modify the vote just before it is sent. The integrity can therefore not be guaranteed. There's also a third problem: as the whole voting process take place on the web platform, the voter has to authenticate himself on the platform. This can lead an attacker to try to steal credentials of voters and to vote for them.

A research group of the Bern University of Applied Science is active since a few years in the e-voting domain. They developed a concept to address the

problem of the secure platform. Further of the publication of this concept, it was decided to make a proof-of-concept in order to check the feasibility of this concept and in order to have a demo tool which could be used in presentations of the concept. The realization of this proof-of-concept was assigned to two students, Andrea Pellegrini and Philémon von Bergen, for their bachelor thesis. A thesis is about 360 hours of work, so that means that this proof-of-concept was done in about 720 hours. The name of the project *SwissiVi* is a composition of "Swiss" and "iVi". "Swiss" comes from the fact that it was developed and will be used in Switzerland. "iVi" is the french pronunciation of the initials of e-Voting, so "e" and "V".

In the next chapter, we will briefly discuss the concept that had to be implemented and have a look on the work that had to be done in this bachelor thesis. We will then present the methods used for the implementation of the different components and then analyze the results. We will finally make a few propositions for future work and ameliorations that could be done.

2 The concept of the Bern University of Applied Sciences

The concept developed by the Bern University of Applied Science addresses the secure platform problem. This concept introduces two additional actors to the web platform, namely a voting card and a voting device. The voting device is a trusted secure device, which means that it can't be manipulated, like being infected by a malware. This design feature can be addressed in a hardware way for example. This concept is shortly described here. It can be studied in greater details in the original publication [1].

2.1 Description of the concept

The concept keeps the use of the web platform, but it is only used to show the different proposals. The vote options for each question, namely yes, no and blank vote, are encoded in three different two-dimensional barcodes. The web platform is not used anymore to send the vote. The vote now is realized on the voting device.

The voting device must at least be equipped with a small display, a numeric key board, a camera and a card reader. It can be shared among several people, for example, a family could use the same device.

The voting card is used to authenticate the voter. It is a personal smart card. It is protected with a PIN code in order to prevent an unwanted use when the card is lost or stolen. The voting card contains personal data about the user as the community and the canton where he lives and cryptographic keys. This card must be a smart card in order to do some computation. The card must be inserted in the card reader built in the voting device. When it is inserted, the device boots up and can be used to vote.

The voting process works as follow: the voter uses his computer to display the web platform. The platform shows the proposals and the vote options encoded in

Fig. 1. Voting process as described in the concept

barcodes. The voter takes a voting device, inserts his voting card in it and scans the barcode representing the vote option he wants to choose with the camera of the device.

Once done, the device writes the question and the selected response on its display and asks the user to confirm his choice. Then, the device encrypts[1] the vote so that the confidentiality of the vote can be assured. The encrypted vote is then sent to the card. The card signs it digitally in order to prevent it from modifications and to authenticate the vote[2]. The card can the be connected to the computer which can be used to recuperate the vote and send it to the bulletin board[3].

Assuming the computer used to show the web platform is still infected with a malware, following issues have been solved:

Confidentiality of the vote The choice made by the voter is done through the scan of a barcode showed on the screen of the computer. So the computer itself has no way to detect which barcode is being scanned.
When sending the vote from the voting card to the bulletin board, the computer is used again. Since the vote is encrypted on the device, it cannot be read when it is sent over internet. The confidentially flaw is solved.

[1] The public encryption key of the bulletin board is used here.
[2] The voting card contains a private key assigned to the voter. The corresponding public key is known by the bulletin board. So, the board can verify that the vote has not been modified after he has been signed, and also that the voter had the rights to vote for this proposal.
[3] The bulletin board is a server where the votes are sent and stored.

Integrity of the vote As the device cannot be infected by a malware, the vote realized on the device is ensured to be correct. However, what could happen is that the malware on the computer swaps the barcode for vote option "yes" and the one for vote option "no". A user scanning barcode for "yes" would vote "no" without wanting it. That's why the voting device shows what was scanned on its display and asks for a confirmation. The user can control if the scan was correct and prevent this attack to occur.

Identity theft Since the voter doesn't need to login on the web platform, there aren't any credentials anymore. To steal the identity of a voter, an attacker would have to steal the voting card and the corresponding PIN code (two factors authentication).

As we can see, every problem mentioned in the introduction is solved by this concept. The only condition that is not respected here is that each voter should only be able to vote once. This problem can however be addressed in the bulletin board, but that's not part of this work.

2.2 Work to do

Having a demonstrator for this concept would help people to understand how this should function. This would really help to convince people that the system is realistic and trustworthy. It would also help people to realize that there is a problem with a single voting platform. The concept specifies how the system must work including the cryptography, but no more. What the implementation of the proof-of-concept must be like was left to the student.

A first main work is to implement a website representing the web platform. This implies the programming of a web page that gets the vote proposal and the candidates for elections in a database and displays them in convenient way. This page must also generate barcodes containing the responses the voter may want to choose. The platform must take the provenance[4] from the voter into account in order to display only the proposal concerning him. Another main task is to implement the voting device and the voting card. Since the hardware for these two components doesn't exist yet, they have to be simulated on smartphones. Each of this two components must be independent, that means that there are two smartphones needed. This also implies that there must be a communication between them. The voting device should be able to read a barcode, make some cryptographic processes like verify a digital signature and encrypt the vote, it should ask for the PIN of the voting card and allow to change this PIN code. The voting card must be able to compute a digital signature on a vote and allow the user to choose the language in which the voting device must display the texts.

Additionally, a simulation of a bulletin board that would allow to control the correctness of a vote has to be developed. That's used to check the proper functioning of the whole system by decrypting the votes and verifying the signatures

[4] In Switzerland, proposals are not the same for each canton or community. So, it is necessary that the voting platform knows the provenance of the voter to display the correct proposals.

and finally by displaying the content of a vote. So, the voter can check if the content of encrypted vote was really what he wanted to vote. In this mean, it's not a real bulletin board in the true sense of the term. It should allow to upload a file containing the vote, decrypt it and verify the digital signature. It doesn't have to store the votes. Once displayed, the votes can be deleted. In parallel, an administration panel for the web platform has to be done. This panel allows to keep the web platform up to date with the actual proposals in a simple way and to manage the database behind the website. That should allow to publish, unpublish and remove voting proposals or add new proposals.

The work was split as follow: Andrea Pellegrini was rather responsible for the web part. That means the voting platform, the admin panel and the bulletin board. Philémon von Bergen was rather in charge of the simulation of the voting device and the voting card. However, there were a lot of interactions between these domains, so it can be considered that the work has be done together.

3 Voting platform

The voting platform is a website that allows the voter to display the actual voting proposals and elections for his community and canton of residence. Since there are four national languages in Switzerland, it is necessary that the webpage is internationalized. So, the first step for the voter arriving on the web platform is to select his language, if it has not been detected automatically. Then the user has to select, on a map or in a list, the canton where he lives (figure 2). He's then redirected to a page where he can indicate his community of residence.

These two steps allow the system to display the voting proposals and elections that concern the voter, in federal level, cantonal level and communal level. For each level, the voter can choose his preferred language, since it could be that the proposals are not proposed in the same language as the interface of the website.

The user can then display the voting page. The three levels are separated in vertical tabs. The proposals and elections for each level are placed in horizontal tabs (figure 3). There's a different interface for voting proposals, initiative proposals[5] and elections. For voting proposals, there are three bi-dimensional barcodes, one for the "yes" response, one for "no" and one for the blank vote. For the two other types, the content of the barcode depends on the selection of the user, so it has to be generated consequently. As we don't want that the voter's selection is sent through internet to the server, the barcodes must be generated on client side. That also means, that if a malware is installed on the computer, it can get information about how the voter voted (for example the list of chosen candidates). However, this is an acceptable compromise, because the malware can easily be tricked in that the user changes his choice a few times, so that the malware cannot know which barcode has been scanned.

A particularity of the web platform is that once the voting page is loaded, the internet connection is no more needed. This ensues from the fact that once the

[5] An initiative is a voting proposal grouping three questions in relation. The voter can independently choose a response for each question.

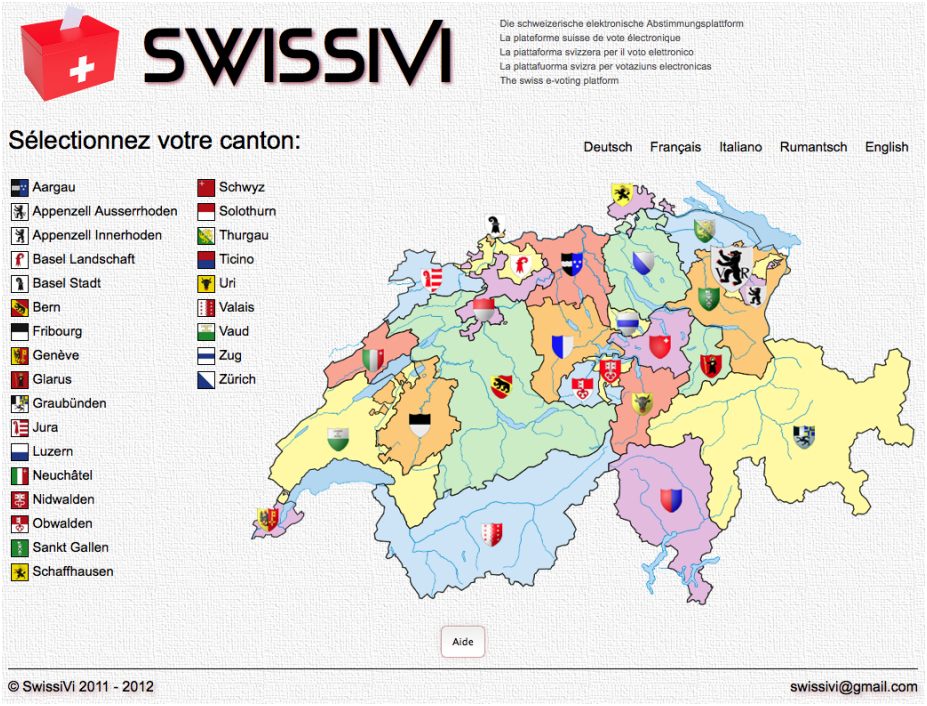

Fig. 2. Home page of the voting platform allowing to select the canton of residence

voting page is generated, all calculations (navigation through the page, barcode generation, selection of candidates and list of candidates) are done in javascript. So, the voter that fears to be spied through internet can disconnect the computer from the network and do the vote process offline.

4 Voting device and voting card

As the hardware for voting device and card doesn't exist yet, these actors have been simulated on two different smartphones. Android was chosen rather than iOS because of the knowledge of the programming language (Java) and the simplified development process. As there are two smartphones, one simulating the card, the other the device, a communication between them had to be implemented. NFC[6] was chosen because the small distance required by this technology represents best the introduction of the card in the device.

[6] NFC means near field communication. It's a communication technology that only works over very small distances (about 2-3 centimeters).

Fig. 3. Voting interface with the vertical and horizontal tabs and the voting options

4.1 Voting device

The simulation of the voting device is based on a state machine that controls the cycles. There are two main processes: the "voting process" and the "change PIN" process. First, the device boots up when it receives the first NFC message from the card (simulating the insertion of the card in the device). Then the user can select one of the two mentioned processes. In the voting process, the first step is to scan a barcode. Once done, the device displays the content of the scanned barcode. The user has to read the text on the display and confirm his choice. The vote is then encrypted. The user is then asked to enter the PIN code of the card. If it is correct, the vote is sent to the card (through NFC). The device waits a confirmation of the card, and shuts itself down. In the "change PIN" process, the standard method is used: asking actual PIN, enter new PIN, confirm new PIN. To manage these cycles and all special cases, the state machine was the best architecture to adopt.

Reading a barcode is done with the ZXing Android application. This app returns the content found in the barcode. The voting device app does the rest of the processing.

4.2 Voting card

The simulation of the card contains one thing more than described in the concept, namely the possibility to choose the language in which the texts on the device must be displayed. Once this chosen, the card sends the first NFC message to the device and then waits for a message from the device like encrypted votes or a change PIN request. In the two cases, it sends a receipt confirmation to the

Fig. 4. Voting device

device. Additionally, in the first case, the card computes a digital signature on the votes and stores them in XML files on the SD card of the smartphone in order to allow the user to retrieve them and to send them to the bulletin board.

Fig. 5. Voting card

In this simulation, the PIN code is chosen randomly at startup of the app and is showed on the display of the smartphone so that the user can read it when it is asked by the device.

5 Results

As the goal of this project was to program a demonstrator for the concept, a special value was placed on the look and feel. As this tool has to convince people about the utility of this concept, it is important that the design looks nice and attractive. Another important parameter was to make the different components as usable as possible. The use of a voting device and a voting card is a bit more complicated than a single voting platform. So, it is important that the device and the card aren't too complicated to use. The voting cycle and the different texts appearing on the device were designed to be easy to understand.

Allmost all the specification defined for the voting device, the voting card and the voting platform have been met. The only exception is the cryptography. In this project, the time was not sufficient to do that. At the moment, the system works without it. The architecture, however, is designed to easily allow a later implementation.

On the other hand, in order to have a good demo tool, it was important to have an administration panel which allows to keep the web platform up to date. It offers the possibility to publish, unpublish or delete voting events, and to import new events from an XML file.

In order to test if the system works correctly, a simulation of a bulletin board was implemented. It allows the user to upload the XML files containing the votes and to check their content. So, this means that it isn't a real bulletin board that would count the votes. It's just a testing tool. If the vote contained in the uploaded file is correct, that means that the content of the barcode of the web platform was correct and that the device and the card have done their job correctly. So, this simulation allows to test the whole voting cycle. A special version of the Android apps named "Standalone version" has been developed to allow to test the system with a single smartphone without NFC capabilities.

All the results can be viewed online under:
https://projects.ti.bfh.ch/swissivi and
https://projects.ti.bfh.ch/swissivi/public/ressources/apps/

6 Future work

As it has been mentioned, cryptography has not be implemented, nor in the device and card, neither in the web platform. Since the goal of this work was to have a demo tool, the focus was placed on the usability and the appearance more than on the cryptography. But an e-voting system without cryptography is not secure, so this implementation would be the next work to do in this project.

At the moment, the voting card and the voting device are simulated on smartphones. A future work would be to develop a hardware for these two components. It would make the project more realistic.

The actual bulletin board is only a simulation. A next step would be to implement a real bulletin board that receives the vote and a tallying system that decrypts and counts the votes. But that's a project for itself.

Finally, verifiability should be implemented in the system. Verifiability means the possibility for a voter to check that the system has done the counting of the votes correctly and the possibility for the voter to check if his vote has been counted. This is important to establish trust in the system.

7 Conclusion

The demonstrator obtained at the end of this project meets the functionality specifications described in the concept as well as the goals of the project. There is working voting card, a working voting device and a usable voting platform. This means the obtained results show that the implementation of the concept is feasible, what also was a goal of this project. The results obtained are more than satisfying for a first implementation. However, they surely could be optimized the day a real implementation is done.

As said in the previous section, the work for a complete e-voting system is not yet done. There are still some missing components. But the implementation of this concept is a step forward to e-voting as it proposes a solution to the "secure paltform problem" and as it is now known that a realization can technically be done. The demonstrator obtained in this thesis has been used in several conferences to present the concept to both technical experts and ordinary people.

The main challenge now will be to convince non-specialist people of the utility of the voting device and the voting card. Their use is more complicated than a single voting platform, but it has real security improvements. We hope, people will understand these reasons and accept to use the system described in this document. We also hope a real implementation of this concept will be done one day. The concept has been presented to the Swiss chancellery. A plan to have an electronic voting system for swiss people living abroad in 2015 is currently being discussed. What type of system will be chosen is not known yet.

References

1. R. Haenni and R. E. Koenig.: Voting over the Internet on an Insecure Platform. In: *Design, Development, and Use of Secure Electronic Voting Systems*, IGI Global, submitted.