Selectio Helvetica: A Verifiable Internet Voting System

Dubuis, Eric; Fischli, Stephan; Haenni, Rolf; Serdült, Uwe; Spycher, Oliver

Edition Donau-Universität Krems

Peter Parycek, Manuel J. Kripp, Noella Edelmann (Editors)

CeDEM11

Conference for E-Democracy and Open Governement

5-6 May 2011

Danube University Krems, Austria

Austrian Federal Ministry of Science and Research

CeDEM11

Proceedings of the International
Conference for E-Democracy and Open Government

BMWF
Austrian Federal Ministry of Science and Research

BUNDESRECHENZENTRUM
BRZ

Conference Website
www.donau-uni.ac.at/cedem

In Cooperation with
OA eJournal of E-Democracy and Open Govnernment
www.jedem.org

Funded by the Austrian Federal Ministry for Science and Research.

Sponsored by the Austrian Federal Computing Centre.

Peter Parycek, Manuel J. Kripp, Noella Edelmann
(Editors)

CeDEM11

Proceedings of the International Conference for E-Democracy and Open Government

5-6 May 2011
Danube University Krems, Austria

Print: Verlagshaus Monsenstein und Vannerdat OHG
Am Hawerkamp 31
48155 Münster
http://www.mv-verlag.de

Publisher: Edition Donau-Universität Krems

ISBN: 978-3-902505-20-0

Donau-Universität Krems, 2011
Dr.-Karl-Dorrek-Str. 30
A-3500 Krems
www.donau-uni.ac.at

Selectio Helvetica: A Verifiable Internet Voting System

Eric Dubuis*, Stephan Fischli*, Rolf Haenni*, Uwe Serdült**, Oliver Spycher***

** Bern University of Applied Sciences, CH-2501 Biel, Switzerland, {eric.dubuis, stephan.fischli, rolf.haenni}@bfh.ch*

*** Centre for Democratic Studies, CH-5000 Aarau, Switzerland, uwe.serdult@zda.uzh.ch*

**** University of Fribourg, CH-1700 Fribourg, Switzerland, oliver.spycher@unifr.ch*

Abstract: *Few governments have introduced electronic voting so far. They are all facing criticism regarding the trustworthiness of their systems. The project "Selectio Helvetica" aims at developing an Internet voting system that can withstand such doubts more easily. It offers full transparency by publishing all the relevant voting data on a public bulletin board. This enables voters to verify the inclusion of their votes and the correctness of the tallying. The underlying cryptographic protocol differs from other protocols since it involves mixing the voters' public signature keys, rather than mixing the votes themselves. This paper introduces the Selectio Helvetica project and the cryptographic protocol in a way that is meant to attract an audience that does not necessarily have much technical background; namely representatives from legislation, jurisdiction, governmental chancelleries and, not least, the electorate itself.*

Keywords: Electronic Voting, End-to-End Verifiability, Hybrid Voting Systems, Public Key Mix-Nets

Acknowledgement: Research supported by the Hasler Foundation (project No. 09037).

Over the past decade, the Internet has enabled providers across all sectors to profoundly improve their services. In particular, online banking services have enjoyed their breakthrough. Just as e-voting technology must do today, e-banking had to withstand doubts. It seems unlikely that doubters have gained their trust by reading the software manuals of their banks. It was rather positive experience over time that made e-banking appear to them to be sufficiently safe. By observing their balance sheets, even doubters were able to verify that their transactions are booked correctly. In the vast majority of cases, things just did not go wrong.

1. Introduction

If e-banking works, why should people distrust e-voting systems? After all, it seems far more tempting for criminals to steal money instead of votes. But is it really? The temptation to commit a crime is generated not only by the pay-off in the case of success. It is also qualified by the probability of the crime actually succeeding. Since banks traditionally provide recurring transaction summaries, customers can always object if they feel their money has been stolen, thus exposing

the crime. Voting providers (governments) are not blessed with any similar mechanism. As a matter of fact, they never needed to convince individual voters that their votes have been considered in the final tally; the voters convinced themselves by observing their ballot slip going into the ballot box while knowing that the box remains under surveillance throughout the rest of the voting procedure. In contrast, a given e-voting system, which requires the electorate to blindly trust in the correct transmission of their ballots, might arouse the temptation of letting some votes disappear. A sophisticated e-voting system will therefore come along with a mechanism that convinces voters that their electronic votes have correctly reached their destination.

Putting an appropriate mechanism in place is unfortunately far from trivial; if it is good at convincing voters that their votes will be counted, it will be good at convincing violent coercers or vote-buyers as well. Furthermore, unlike customers in e-banking, voters do not only consider the destiny of their own ballots. While bank customers pay no attention to their neighbors' transactions, voters will want to be convinced that the final tally properly reflects the electorate's will, or technically speaking, that the ballot box contains ballots cast by eligible voters only, and one at most. An e-voting system that requires the electorate to blindly trust in the content of the ballot box being correct, might invite criminals to add extra votes for their favorite candidate.

The few governments that have introduced e-voting so far are facing criticism regarding the trustworthiness of their systems (Schryen & Rich, 2009). *Selectio Helvetica* (SH) is a project aiming at developing an Internet voting system that can withstand such doubts more easily. In particular, it is designed to solve the hard problems that have been described so far, while maintaining the secrecy of the ballot.

This paper describes the SH system and outlines its security features along with potential pitfalls. Apart from the e-voting research community, it is meant to attract an audience that does not necessarily have much technical background; namely representatives from legislation, jurisdiction, governmental chancelleries, and not least, the electorate itself. We thus hope to integrate potential stakeholders into the assessment of contemporary e-voting techniques in general, and the presented scheme in particular. The objective of such an assessment is an operative e-voting system that fulfills legal requirements, complies with voting traditions, and has well-analyzed security properties, which all stakeholders can understand and declare as sufficient.

SH is currently being developed at the Bern University of Applied Sciences (BFH) in Switzerland. A preliminary version of the SH system has been employed by *Baloti.ch*. This is an Internet voting platform for Swiss migrants provided by the Centre for Democracy Studies (ZDA) in Aarau.

2. Electronic Voting and Cryptographic Primitives

For an e-voting system to be secure, it has to function without vulnerabilities in potentially insecure environments such as the Internet. By *insecure environment* we mean that the existence of malicious individuals (or co-operating groups of malicious individuals) is assumed throughout the whole system. For example, it is assumed that network traffic is intercepted, system administrators are corrupt, voters try to cheat, computers are infected by malware, etc. For an e-voting system to work properly even under such unideal circumstances, it has to be implemented according to an intrinsically secure design. As a guideline for designing and implementing such a system, the literature on e-voting technologies offers a whole catalogue of *general security requirements*, which the system should satisfy under all possible scenarios (Cranor & Cytron, 1996, and Nielsen & Andersen & Nielson, 2005). The key instrument for establishing these requirements is cryptography. Below we will informally introduce the most important of these requirements and corresponding cryptographic primitives. Some of these primitives will also be used in the SH system.

Privacy

An e-voting system is private if no vote cast can be linked to its voter, neither by voting authorities nor anyone else (anonymity), and if no voter can prove that he or she voted in a particular way (receipt-freeness).

As a first measure, privacy is established by encrypting the vote before casting it. The voter's particular candidate choice is thus converted into a *ciphertext* to prevent unauthorized third parties from reading it. The encryption key is the so-called *public key* of the voting authority and is publicly known, while the corresponding *private key* may later be used to decrypt the vote. Note that different encryptions of the same candidate choice should not result in exactly the same ciphertext, since this would obviously spoil the anonymity of the vote. It is thus crucial to employ a *randomised* encryption scheme, which individualizes each encryption with a random value.

To perform the final tallying, votes are decrypted individually before performing the actual tallying. To avoid the possibility that a link to the voter can be established easily after performing the decryption, we may employ a *re-encryption mix-net* to shuffle the encrypted votes. In addition to altering the positions of the votes in the list, shuffling also includes *re-encrypting* them. As a result, no link between the input and output of the mix-net can be established, which finally guarantees the anonymity of the vote. In addition to shuffling and re-encrypting, the mix-net must also provide a cryptographic proof of doing so correctly.

Receipt-freeness is one the most difficult requirements, for which no general cryptographic solution exists. In the context of a *hybrid voting system* (Spycher & Haenni & Dubuis, 2010), however, the problem is solved by exploiting traditional paper-based voting channels.

Fairness

A system is fair if no intermediate results can be obtained before the voting period ends.

Using an encryption scheme as explained above does not prevent the voting authority, which is in possession of the private decryption key, to perform a decryption before the end of the voting period. This problem can be avoided by splitting up the private key into several *key shares* and by distributing them among several independent tallying authorities. So-called *threshold secret sharing schemes* allow a shared secret (the private key in this case) to be re-constructed by any group of t (for threshold) or more share owners, but such that no group of fewer than t share owners can. In a *threshold cryptosystem*, it is even possible for a group of t or more share owners to decrypt a given ciphertext without actually re-constructing the private key. Under the assumption that fewer than t tallying authorities are malicious, this obviously asserts the voting system to be fair.

Democracy

An e-voting system is democratic if only eligible voters can vote (eligibility) and if eligible voters can only vote once (uniqueness).

To exclude unauthorised individuals from voting, most systems assume some sort of *voter credentials*, which are distributed to the electorate during registration. The credential is usually a secret random value with an associated public part; for example, a private and public signature key. To prove eligibility, voters must use the credential to digitally sign the encrypted vote. By verifying digital signatures, one can check if votes cast originate from registered voters and whether they are unique.

Accuracy

An e-voting system is accurate if votes cast cannot be altered (integrity), valid votes cannot be eliminated from the final tally (completeness), and invalid votes are not counted in the final tally (soundness).

During transmission to the voting server, the integrity can easily be ensured by letting voters digitally sign their votes cast. However, these signatures must be removed (or disguised) at some point to allow the anonymization of the votes. From then on, the vote will no longer be under the voter's control. Nevertheless to establish trust in the accuracy of the tally, voting systems are required to be verifiable.

Verifiability

An e-voting system is individually verifiable if voters can independently verify that their own votes have been counted correctly in the final tally. A system is universally verifiable, if voters can independently verify that all votes cast are from legitimate voters and that they have been counted correctly in the final tally. Individual and universal verifiability together is sometimes called end-to-end verifiability.

Verifiability is usually achieved by publishing all votes cast (together with corresponding cryptographic proofs) on a public *bulletin board*. Voters can read the content of the board and post new entries (possibly to their own board sections), but nobody can delete or change anything. In this way, voters are able to individually verify the inclusion of their votes and to re-compute the result of the tallying. The general idea is to make the voting system completely transparent by publishing all the relevant voting data. The security of the system is thus fully protected by cryptographic means instead of technical or procedural measures.

3. Selectio Helvetica

The Selectio Helvetica (SH) project aims at developing an Internet voting solution that complies with the crucial security properties. Furthermore, it is designed to potentially serve as the electronic channel of a hybrid voting system with regard to the Swiss political context (Spycher & Haenni & Dubuis, 2010). Although it is not planned to be immediately employed for political elections and referendums, SH will provide Internet voting services to non-governmental voting organizers, thus offering a proof of concept. The Baloti project (see Section 4) has already run three referendums using the preliminary version of the SH system. The voter-verifiable implementation discussed here is scheduled for operation in fall 2011.

Section 3.1 introduces the cryptographic protocol that underlies SH. It explains the basic security properties under the restriction that voters can receive their personal voting credentials through a privacy-preserving channel that guarantees the voters' authenticity (authenticated channel). This restriction seems reasonable, given that governments will offer an infrastructure for distributing them. In contrast, the budgets of non-governmental voting organizers can be tight. Therefore, SH involves e-mail for distributing credentials. Section 3.2 explains how the SH system works under an extension of the underlying protocol.

3.1. The Selectio Helvetica Protocol

The underlying protocol is a modification of the one introduced in (Spycher & Haenni, 2010). Due to space constraints, the present paper leaves the secure vote revocation protocol of the hybrid system undiscussed.

First Approach

Digital signatures offer a common way of ensuring the authenticity and integrity of messages. If Mrs. Smith signs a message using her private signature key S, the receiver Mr. Ryan can convince himself that the sender of the message is not an imposter, who just claims to be Mrs. Smith. To do so, he uses Mrs. Smith's public signature key S and compares it with the message's signature and the message itself. Given that Mr. Ryan believes that Mrs. Smith keeps her private signature key S to herself, he is assured about the origin of the message, if the result yields a match.

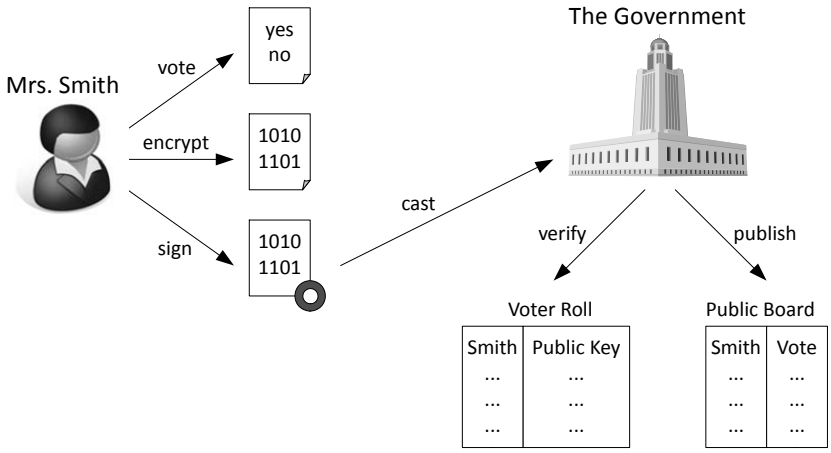

Figure 1: Simplified Internet Voting

The technique of digital signing can be employed in Internet voting as well. Imagine Mrs. Smith is a voter and Mr. Ryan is the government. The government holds the voter roll enlisting all eligible voters, including Mrs. Smith. For the purpose of Internet voting, the voter roll is published on the Internet, showing each of its entries coupled with the voter's public signature key S, which the government uses to verify the authenticity of messages. When Mrs. Smith wants to cast her vote, she enters her candidate choice in the computer, which encrypts her vote using the government's public key. The result is the message she is about to send to the government. Since only the government can decrypt her message, she does not need to fear that any curious people on the Internet can find out how she voted. To convince the government that her vote should be counted, Mrs. Smith enters her private signature key S into her computer to generate the signature of her message and sends both to the government. After receiving her message, the government verifies that the sender of the message is Mrs. Smith by comparing the signature with the message using her public key S. Since she is enlisted in the voter roll, the government will know that it needs to decrypt her vote and count it. However, before decryption, the government should wait until the voting phase is over (fairness). Furthermore, it needs to apply a re-encryption mix-net on the set of all collected votes, in order not to learn how Mrs. Smith voted (privacy).

Discussion

The simplified scheme presented holds a number of obvious and maybe not so obvious pitfalls. These are discussed in the following Q&A section.

Q: *How can voters be certain that the government does not secretly decrypt their votes before applying the re-encryption mix-net?*

A: The full protocol requires a majority t of authorities to participate at the decryption (threshold cryptosystem). This implies that one authority alone cannot decrypt any votes. In fact, even no coalition of less than t conspiring authorities has a chance at decrypting Mrs. Smith's message. If it seems reasonable to assume that a majority of the authorities will refrain from being dishonest, the described measures ensure the voters' privacy and prevent premature decryption of votes.

Q: *How can voters verify that all and only legitimate votes are counted?*

A: The authorities' environment publishes the electronic ballot box, which comprises the set of all collected votes (public bulletin board). If Mrs. Smith ever believes that her vote might not have reached the electronic ballot box or that it has been deleted from there, she can always verify that her vote is correctly enlisted by downloading a copy of the electronic ballot box (individual verifiability). By additionally downloading a copy of the electronic voter roll and verifying all signatures of the encrypted votes and the zero-knowledge proofs provided by the mix-net, she verifies that all and only legitimate votes are counted (universal verifiability).

Q: *If voters reveal their identity by signing their encrypted votes, they declare to the public that they have participated at the vote. Furthermore, voters that do not participate are publicly exposed.*

A: In the full protocol, the public keys used for verifying signatures are mixed prior to the voting phase (using a *public key mix-net,* which is similar to a standard re-encryption mix-net). Thus, Mrs. Smith can still sign her message by using the same private signature key s , while the verification of the signature is done by using her anonymous public key $\tilde{s}$, called her pseudonym. Since the correctness of the public key mix-net is verifiable by downloading the corresponding zero-knowledge proofs, universal verifiability remains in place.

Q: *If voters can verify that their votes are counted correctly, they can prove to vote-buyers and coercers how they voted. Moreover, voters can even hand out their private signature key s , although they are supposed to keep it to themselves.*

A: This is true if the SH protocol is used as a stand-alone voting channel. However, vote-buying and coercion are mitigated by requiring voters to revoke and overrule their electronic vote at the polling station (hybrid system). In the case that no polling stations are available, the SH scheme is clearly not coercion-resistant. We believe that this is unproblematic as long as SH is used as a proof of concept for non-governmental voting events.

Q: *If the voters' computers run viruses, they might display corrupt information at verification and mislead voters.*

A: This is true. The so-called *trusted platform problem* needs to be addressed independently of the presented protocol. Whether the available counter-measures suffice is a matter of dispute and requires thorough analysis.

Concise Description

The full protocol assumes two groups of players (*voters* and *authorities*), the existence of a voter roll, an initially empty public bulletin board, an anonymous channel for casting the votes, and a secure authenticated channel between authorities and voters.

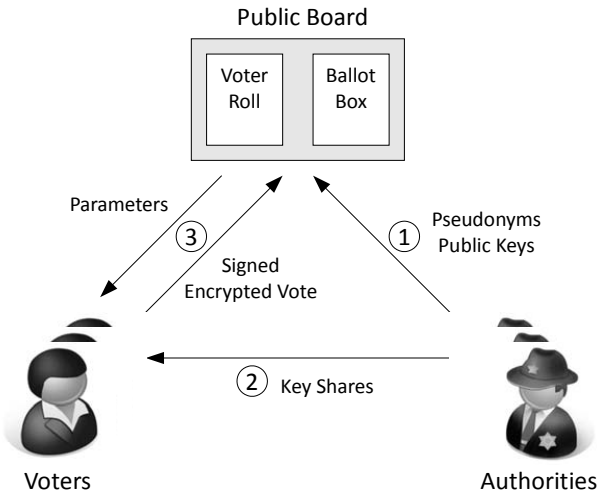

Figure 2: The SH protocol

The protocol is divided into four phases:

1. *Setup*: The authorities jointly generate a signature key pair (s, S) for each potential voter, mix the public keys S into pseudonyms $\hat{S}$, and generate a shared encryption key. All these parameters are published on the public board.
2. *Voter Registration*: A voter is associated to an unused public signature key S. The authorities send their shares of the corresponding private signature key s to the voter. The voter reconstructs the private key from the shares.
3. *Vote Casting*: The voter requests the relevant parameters and keys from the public board, encrypts the vote using the public encryption key of the authorities, signs the vote using the private signature key s and sends it together with the computed pseudonym $\hat{S}$ back to the public board.
4. *Tallying*: The authorities use their shared private keys to decrypt the votes, for which the signatures hold against valid pseudonyms. The results are published on the public board.

Since the public board contains all proofs required by the primitives described in Section 2, the public can verify that all and only legitimate votes are counted. By using their private signature keys s to compute their pseudonyms, voters can verify that their votes have been decrypted as intended.

3.2. The Selectio Helvetica System

The outlined protocol is primarily designed to run governmental votes. The SH system is meant to constitute a proof of concept of that protocol by running an Internet voting service for non-governmental vote organisers. Since they tend to operate on lower scale budgets, they do not necessarily run an infrastructure that includes a secure authenticated channel to transmit the shares of voters' private signature keys in a user-friendly way (step 2 of the protocol). Similarly, vote organisers will not usually offer any hardware, such as smart cards for voters to easily store and read their private keys. Further, in contrast to the assumption of the protocol, vote organizers

do not necessarily own a final voter roll prior to the beginning of the voting phase. The SH system is meant to address these restrictions.

Instead of requiring voters to save their very long, unintuitive private signature keys, in the SH system they request their shares from the authorities each time they need it for computations. Whenever voters need their private signature keys, they simply enter a password that they have chosen themselves at registration.

Extension of the Protocol

The extended protocol underlying the SH system involves two additional players. The vote organizer assesses the voter's right to vote. The voting provider acts as an intermediary among voters and authorities, and writes to the public board.

The registration phase is extended as follows: A voter first asks the vote organizer to sign his e-mail address in order to confirm that he is enlisted in the voter roll. The voter then sends the signed e-mail address to the voting provider. He by return associates the voter's e-mail address with an unused public key S on the public board and sends the registration credentials back to the voter by e-mail. (Instead of the e-mail address a nickname chosen by the voter could be published.) The voter chooses a password and uses it to compute one designated hash code per authority. These hash codes are sent to the authorities along with the registration credentials. The authorities verify the credentials and map the hash code to their share of the private signature key s corresponding to the voter's public signature key S .

Whenever an authority receives a request with a valid hash value, it replies with the share of the private signature key s mapped to it. Thus, if voters want to cast their vote, they only have to enter their password.

The other phases of the SH system follow directly from the original protocol.

Employed Technologies

The SH system is implemented using only well-defined, widely used, and standardized technologies. Components communicate through *web services*. Since web services are based on XML, the components can be implemented and operated on any platform, such as Java EE or .NET. Furthermore, communication channels are secured on the transport layer using HTTPS.

The usability and performance features of the components used by the voters are crucial. At the same time, a technology must be used which is available on virtually all potential computers used by voters. This is addressed by letting voters use web browsers running JavaScript and Java accessed through LiveConnect.

The server-side components are implemented using the Java EE platform and operated on a JBoss application server. In addition to the core functionality, each component has been enhanced by a management console, which allows to initialize and monitor the components during operation.

4. The Baloti Project

On the Internet platform *Baloti.ch* the migrant population living in Switzerland can cast votes with the help of Selectio Helvetica. A public call for integration projects by the Swiss Federal Commission for Migration Issues allowed an interdisciplinary consortium to design and test a multilingual Internet platform mimicking Swiss referendum politics as a two year pilot starting in 2010. Besides politically neutral information on current referendum votes, the website offers a replica of a ballot vote for all issues at stake on the Swiss national level and thus provides a test-

bed environment for electronic voting. Because of the political nature of the project and the sensitive information (political preferences) that is passed on from the web browser to the electronic urn, it was important to provide a secure Internet voting system. In order to build up trust in the system, we opted against having a user registration and a permanently stored user profile.

In order to understand the motivation behind the project, three points of background information should be taken into account:

- The Swiss political system allows its citizens to vote not only on the occasion of elections but also on concrete issues three to four times a year on all three state levels (national, cantonal, local). A ballot can be triggered automatically in case of constitutional matters or by the collection of a certain amount of signatures. The vote can block legislation (referendum) or suggest new provisions (initiative). These various mechanisms of direct democracy can affect the constitution, international and domestic treaties, laws as well as ordinances and thus touch the people's life in many respects, whether they have Swiss citizenship or not.
- At 22 percent, the population of migrants living in Switzerland is comparatively high. To gain full citizenship and voting rights migrants can start a naturalization procedure after twelve years of residence. In practice, a large part of the population is thus not fully integrated in the political life of the country. Whereas most of the French speaking cantons have given migrants voting rights on the local and/or cantonal level, respective initiatives have mainly been turned down in the Italian and German speaking cantons. However, a few German speaking cantons allow their communes to introduce political rights for migrants at their own will (e.g. Appenzell Ausserrhoden, Grisons).
- The three cantons of Geneva, Neuchâtel, and Zurich are testing Internet voting systems for several years now (Serdült, 2010). However, only 10 percent of the total population is allowed to participate in these Internet voting experiments. That is the reason why in practice Internet voting in the three cantons is restricted to a couple of pilot communes. In addition to the resident citizens, Internet voting is on the way to being made available to all Swiss living abroad by 2015. Henceforth, there is an increased interest and demand for applied research on the topic of secure Internet voting.

The main motivation of Baloti.ch is therefore to grant migrants living in Switzerland the opportunity to familiarize themselves with the Swiss political system in a novel and realistic way. On our platform migrants can practice direct democracy in the eleven most spoken languages in Switzerland (German, French, Italian, English, Spanish, Portuguese, Turkish, Albanian, Serbian, Croatian, and Tamil). With Baloti.ch we therefore contribute to the political integration of migrants. Whereas migrants without voting rights constitute the most important target group, the website can also be useful for the Swiss living abroad, for young Swiss citizens under 18 and for civic education purposes in schools in general.

The goal of the pilot is threefold: Firstly, migrants living in Switzerland without voting rights are granted an opportunity to manifest themselves politically. The results of the vote are displayed almost the same hour when the official vote closes and is further communicated via Facebook and Twitter. Secondly, visitors of the platform can learn how direct democracy works and practice it one to one. Baloti.ch therefore helps to bridge the twelve years until the naturalization process can eventually be started. Thirdly, at least ideally, the political will of the migrant population is made transparent. In the research part behind the project we would like to find out whether the voting behavior of migrants differs significantly from the one of Swiss voters. As a working hypothesis we expect the differences between the two groups to be minimal as soon as a reasonably high number of migrants starts voting on Baloti.ch.

Baloti.ch is activated three weeks before a national referendum vote. This three week period corresponds to the time span Swiss citizens are allowed to cast their vote. During the voting period the electronic ballot box on Baloti.ch is open and information on all national votes is displayed (content of the vote at stake, arguments in favor and against the bill, recommendations by political parties, parliament and the government). All initial text material is provided by one of our partners (Vimentis) in German, slightly adapted and then carefully translated by an external team. The translators are all native speakers, and all translations are subject to the four eye principle.

With the help of press releases, coverage on Swiss TV and radio stations, Facebook and Google Ads, contacting migrant organizations as well as all official competence centers for migration issues throughout the country Baloti.ch was advertised and went online for the first time during the September 2010 vote on a revision of the Swiss Unemployment Insurance Law. Voters had ten days to cast their vote (16^{th} to 26^{th} of September 2010). During that time span the website had 3'300 single visitors (according to Google analytics). Roughly 10 percent of all visitors cast a vote by first obtaining a voting credentials by e-mail and then deciding whether to be in favor or against the bill. 60 percent of the Baloti voters opposed the bill whereas the official result of the Swiss citizens showed a 53 percent acceptance. For the second Baloti vote in November 2010 the website had 4'500 visitors but fewer votes than in September 2010. Only 240 visitors bothered to cast a vote. The decrease of cast votes could partly be attributed to the complicated nature of the bills and several pending usability problems. During the remaining time of the pilot until the end of 2011 we will address these issues and constantly improve the site.

5. Discussion and Conclusion

The SH protocol and system have been presented on an introductive level. Although there are secure solutions to questions like what happens if users forget their passwords or how do voters handle corrupt shares of their private signature key s , they are out of the scope of this paper. Not letting anyone know how voters have voted, not even letting anyone know whether they have participated, being able to detect fraud, even in the case of all authorities being corrupt, summarize the strong features of this protocol. Mathematically proving the positive security features of SH is left to a more formal paper. Instead, we aim at including a broad audience of stakeholders in the assessment of e-voting technology. In that spirit, we outline some critical issues for discussion.

- Trusted Platform: A computer that runs viruses can cast corrupted votes and mislead at verification, or send private information to third parties. Which measures need to be applied to optimally and sufficiently address the problem?
- Integrity: In case verification fails, voters can re-submit their vote until they witness a correct encryption of their vote on the public board. Does this comply with the superior legal constraints?
- Coercion-Resistance: Within the containing hybrid system, coercion is mitigated by allowing voters to securely revoke (i.e., the correct vote gets excluded while privacy remains in place) and overrule their vote at the polling station. Is this a sufficient measure to address vote-buying and coercion?
- Dispute: To avoid disputes, voting providers could declare it the voters' responsibility to verify that their vote has been cast correctly using a trusted platform. In case re-submitting the vote does not help, they are required to revoke and overrule their vote at the polling station. Is this feasible, considering that voters do not participate at every vote?
- Privacy: Voters do not necessarily trust the privacy inducing measures of the administration's software and processes. By defining multiple authorities, voters merely need to trust in a majority of the organizations working correctly, which is clearly an improvement. But is it sufficient?

- Privacy: The cryptographic measures that induce privacy on the public board will sooner or later be broken. Is it a problem if the public learns how their ancestors voted 100 years ago?

We see SH as a starting point to debate these open questions in more specific terms.

References

Cranor, L. F., & Cytron, R. K. (1996). Design and Implementation of a Practical Security-Conscious Electronic Polling System. *Technical report, WUCS-96-02*, Washington University.

Nielsen, C. R., & E. H. Andersen, & E. H., Nielson, H. R. (2005). Static Validation of a Voting Protocol. *Electronic Notes in Theoretical Computer Science, 135(1)*, 115-134.

Schryen, G., & E. Rich, E. (2009). Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and Security, 4(4)*, 729-744.

Serdült, Uwe (2010) Internet Voting for the Swiss Abroad of Geneva: First Online Survey Results, in: Chappelet, Jean-Loup et al. (Eds.) *Electronic Government and Electronic Participation: Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2010*, Schriftenreihe Informatik, 33, Linz, Trauner Verlag, 319-325.

Serdült, Uwe (2010) Baloti Abstimmungs-Report für die eidgenössischen Abstimmungsvorlagen vom 26. September 2010: Revision der Arbeitslosenversicherung (ALV). Aarau, Zentrum für Demokratie Aarau ZDA.

Spycher, O., & Haenni, R. (2010). A Novel Protocol to Allow Revocation of Votes in a Hybrid Voting System. In proceedings of *ISSA'10, 9th Annual Conference on Information Security - South Africa*, Sandton, South Africa.

Spycher, O., & Haenni, R, & Dubuis, E. Coercion-Resistant Hybrid Voting Systems. In R. Krimmer and R. Grimm (Eds.), *EVOTE'10, 4th International Workshop on Electronic Voting* (pp. 269-282), Lecture Notes in Informatics, volume P-167. Bonn: Gesellschaft für Informatik E.V.

About the Authors

Eric Dubuis

Eric Dubuis is professor at the Bern University of Applied Sciences, department of Engineering and Information Technology. He teaches applied security for distributed systems and Web services. His research interests include e-voting systems in general and applied crypto protocols in particular. Currently, he represents the e-voting group of the Bern University of Applied Sciences, and he is co-founder of the Swiss E-Voting Competence Center. He got his PhD degree from the ETH Zürich.

Stephan Fischli

Stephan Fischli is professor for computer science at the Bern University of Applied Sciences. His main interests are distributed systems and software architecture. Since 2008 he is also member of the e-voting research group. He got his PhD degree in mathematics from the University of Bern.

Rolf Haenni

Rolf Haenni is professor at the Department of Engineering and Information Technology of the Bern University of Applied Sciences, Switzerland. He received his diploma and PhD degrees in Computer Science from the University of Fribourg, Switzerland. He is a former visiting scholar at the University of California in Los Angeles, a former research fellow at the University of Konstanz, Germany, and a former assistant

professor at the University of Bern, Switzerland. He has a strong research background and publication record in areas such as probabilistic and logical reasoning, knowledge-based systems, uncertainty management, information theory, knowledge representation, reliability theory, model-based diagnostics, trust management, cryptography, and electronic voting.

Uwe Serdült

Uwe Serdült is vice-director of the Centre for Research on Direct Democracy. He holds a doctoral degree in Political Science from the University of Zurich. He worked as a senior researcher and lecturer the ETH Zurich, and Universities of Zurich and Geneva. Research stays led him to Japan and the USA. In the field of e-democracy he works on e-voting and the long term effects of ICTs on political systems. Ongoing research in the field includes further development of internet based platforms and tools for citizens, public administrations in order to enhance transparency and deliberation in an information society.

Oliver Spycher

Oliver Spycher graduated MSc in Computer Science at the University of Berne in 2007. From 2007 to 2009 he had a position in industry as a test manager, later site manager in Switzerland and Dubai, respectively. Since September 2009, he has a position as a research assistant and PhD student at the Informatics Department of the University of Fribourg in Switzerland, and a position as a research assistant at the Department of Engineering and Information Technology of the Bern University of Applied Sciences (BFH-TI), Switzerland. His main research interest lies in the area of electronic voting.