E-Voting Web Client for OpenCHVote

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisors: Prof. Dr. Rolf Haenni, Prof. Dr. Philipp Locher
Expert: Ciril Saner

Remote e-voting has many benefits in terms of convenience and efficiency. For example, a voter could submit their ballot from anywhere on the planet, simplifying the voting process for Swiss citizens living abroad. In this thesis, we describe the implementation of the client component of such an e-voting system, OpenCHVote.

E-Voting

Although there are many advantages to e-voting, there are also several challenges that need to be addressed. The use of digital systems to enable electronic voting comes with a risk of election fraud. If malicious actors can tamper with the election results or break the secrecy of ballots, trust in democracy is undermined. The „Swiss Federal Chancellery“ formed the „Ordinance on Electronic Voting“, which specifies the requirements for electronic voting in Switzerland.

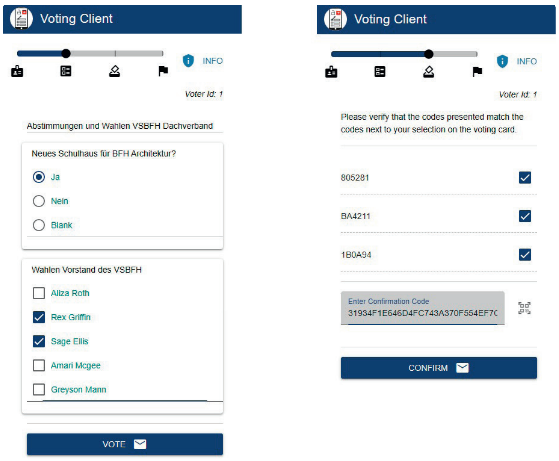
In 2016, the State of Geneva launched CHVote, an electronic voting protocol that satisfies the posed security requirements. With the help of cryptographic codes, voters can determine whether their vote has been registered correctly by the system and that no illegitimate manipulation has occured. The codes are printed on a personalized voting card and sent to each voter before an election takes place. OpenCHVote is the corresponding reference implementation maintained by researchers of the „E-Voting Group“ at BFH. However, it currently does not offer a production-ready voting system. At the time, all the protocol steps and messages are only simulated on a single machine. Furthermore, a critical missing piece of OpenCHVote is a web-based implementation of the Voting Client. It is the primary interface used by voters interacting with the voting system.

Methods

This thesis aims to implement a CHVote compliant voting client so that it can be integrated into the OpenCHVote project. We explore the vital aspects of implementing a cryptographic protocol, especially in the e-voting field. Developing the component from scratch in another programming language proves that the current system functions correctly in a heterogeneous environment. With the prevalence of mobile devices, we employ a mobile-first approach, to assess the usability of the protocol on mobile platforms. A particular focus on the audibility of the code is given by closely aligning the implementation with the pseudo-code. This allows auditors to quickly verify the compliance of the code with the protocol specification. We optimized the performance of the expensive cryptographic operations to provide a pleasant user experience.

Results

Our main contribution is a JavaScript implementation of all cryptographic algorithms necessary for the Voting Client and the protocol state machine. As a result, the voting procedure can be carried out with high security parameters in less than a minute. Furthermore, to improve user friendliness, we suggest and incorporate protocol extensions that account for errors induced by the Voting Client or the Voter. Moreover, we built a user interface that allows voting and viewing election results. Finally, we propose an API specification, which defines end-points, message format, and serialization method for the communication between the Voting Client and the other parties. With this thesis, we demonstrate how the e-voting experience may look like in the future.



Abstimmungen und Wahlen VSBFH Dachverband

Neues Schulhaus für BFH Architektur?

- ● Ja
- ○ Nein
- ○ Blank

Wahlen Vorstand des VSBFH

- □ Aliza Roth
- ☑ Rex Griffin
- ☑ Sage Ellis
- □ Amari Mcgee
- □ Greyson Mann

Please verify that the codes presented match the codes next to your selection on the voting card.

- 805281 ☑
- BA4211 ☑
- 1B0A94 ☑

Enter Confirmation Code: 31934F1E646D4FC743A370F554EF7C

Voting Procedure

Alain David Peytrignet

Elias Johannes Calesanz Schmidhalter