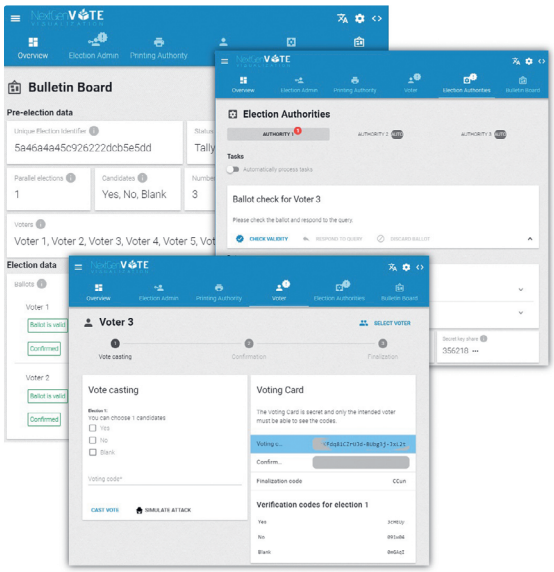
Visualizing Geneva's Next Generation E-Voting System

Degree programme: BSc in Computer Science | Specialisation: IT-Security
Thesis advisors: Prof. Dr. Rolf Haenni, Prof. Dr. Philipp Locher
Expert: Han Van der Kleij (SBB)

With the ongoing digital transformation, it seems only a matter of time until submitting paper ballots is replaced with e-voting. However, secure cryptographic e-voting protocols are known to be notoriously challenging to design and not easy to be understood. For our bachelor thesis, we implemented the protocol on which Geneva's next e-voting system will be based, and built an application that makes it possible to interactively experience the next-generation e-voting protocol

Context

Previous attempts to introduce e-voting platforms in Switzerland were limited to only small electorates as these platforms did only meet the basic requirements set up by the Swiss government. In 2017, researchers from the Research Institute for Security in the Information Society (RISIS) published their specifications for Geneva's new e-voting system, CHVote, which has the potential of being accepted as a large-scale, nationwide e-voting platform. However, one challenge that still remains is the educational problem: it is difficult to understand such a complex protocol without sufficient knowledge of cryptography. This might also result in mistrust towards e-voting.



Goal

The goal of this project is to develop an application that addresses the difficulty to impart knowledge regarding e-voting. Through this project, users will be able to get a hands-on experience with an e-voting system. This would allow a better understanding of the next-generation e-voting protocol. The system will also allow to display multiple perspectives of an election event on different screens, which requires real-time synchronization of data. Another goal is to enable the authors of the specification, our supervisors, to use our application to present and explain their protocol to an audience.

Design and implementation

We first implemented approximately 60 algorithms that have been described in the specifications. In addition to this crypto-library, we also built a back-end that provides the voting functionality as an API. Both the library as well as the back-end are written in Python. Our front-end that visualizes all the voting phases is a single-page application written in JavaScript using the VueJS framework. In order to achieve real-time updates, we have used web sockets (socket.io) to synchronize a client-side copy of the database whenever the data has been altered on the back-end. An intuitive, clean layout and presentation of the data has been one of the biggest challenges in this project.

Results

With our application, it is possible to conduct election events according to the protocol specifications not only from the perspective of a voter, but also all other participating actors such as the election administrator, printing or election authority. Our application combines modern technology and an intuitive design to allow users to gain a better understanding of the protocol and offering a preview of how the future of voting might possibly look like in Switzerland.

Yannick Pascal Denzer

Kevin Marc Häni
+41 79 638 58 18
kevin.haeni@gmail.com