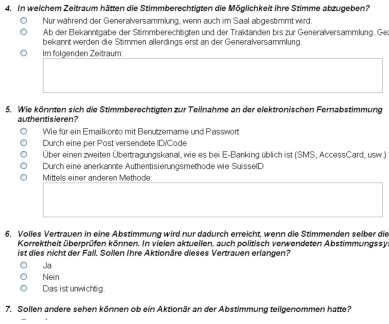
Christoph Galliker

Graduate Candidate	Christoph Galliker
Examiner	Prof. Dr. Andreas Steffen
Co-Examiner	Prof. Dr. Andreas Steffen
Master Research Unit	Software and Systems

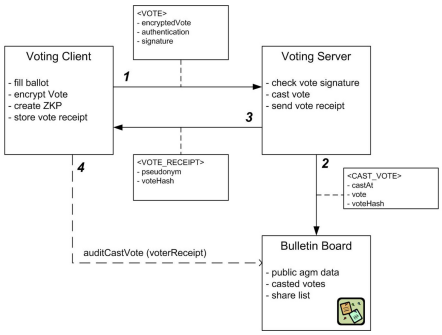
E-Voting for Shareholder Meetings

A basic concept for an end-to-end verifiable internet voting application usable for Annual General Meetings of public companies.

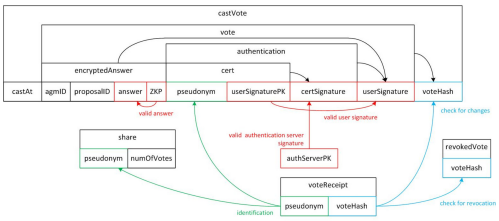


4. *In welchem Zeitraum hätten die Stimmberechtigten die Möglichkeit ihre Stimme abzugeben?*
   - Nur während der Generalversammlung, wenn auch im Saal abgestimmt wird.
   - Ab der Bekanntgabe der Stimmberechtigten und der Traktanden bis zur Generalversammlung. Gezählt und bekannt werden die Stimmen allerdings erst an der Generalversammlung.
   - Im folgenden Zeitraum:
5. *Wie könnten sich die Stimmberechtigten zur Teilnahme an der elektronischen Fernabstimmung authentisieren?*
   - Wie für ein Emailkonto mit Benutzername und Passwort
   - Durch eine per Post versendete ID/Code
   - Über einen zweiten Übertragungskanal, wie es bei E-Banking üblich ist (SMS, AccessCard, usw.)
   - Durch eine anerkannte Authentisierungsmethode wie SuisseID
   - Mittels einer anderen Methode:
6. *Volles Vertrauen in eine Abstimmung wird nur dadurch erreicht, wenn die Stimmenden selber die Korrektheit überprüfen können. In vielen aktuellen, auch politisch verwendeten Abstimmungssystemen, ist dies nicht der Fall. Sollen Ihre Aktionäre dieses Vertrauen erlangen?*
   - Ja
   - Nein
   - Das ist unwichtig.
7. *Sollen andere sehen können ob ein Aktionär an der Abstimmung teilgenommen hatte?*

A completed survey shows what Swiss corporations think about Internet voting for general meetings.



After successful authentication, the shareholders can cast their votes.



All participants are able to verify the correctness of the cast votes.

The Annual General Meeting gives shareholders the opportunity to decide about the future of the company by making use of the their right to vote. Today, vote casting is done by attending the meeting in person or by delegation to another shareholder or a proxy who attends the meeting. The current trend of doing things electronically e.g. e-banking kindles the request to allow vote casting over the Internet. Designing such an Internet voting system one has to consider the special security requirements. In an electronic system if an attacker is able to manipulate votes, she can do this much more easily than a in traditional voting process and thus change the final result of the voting.

In end-to-end verifiable voting systems the voter herself is able to verify that her vote has been accounted for and cast correctly. Next to verifiability, the requirement of the privacy of votes must be fulfilled. To achieve this objective, the ballots must be encrypted by use of modern cryptographic techniques. This project thesis analyzes if and how an end-to-end verifiable voting system can be used in the context of shareholder meetings in order to enhance both security and privacy. This comprises the establishment of a coarse requirement specification for such an e-voting system. Beside some literature study, the requirements base on a survey, where different Swiss companies were polled on the idea of such a voting system. Furthermore the thesis includes a proposal for a basic concept of the voting application and the way it could be realized with the Paillier cryptosystem. Thus common cryptographic techniques such as Homomorphic Tallying, Zero Knowledge Proofs and the distributed generation of Paillier private keys are examined.

The designed concept is prepatory work for a master thesis to be completed during the spring semester 2011. My colleague Halm Reusser and I will develop and implement a basic version of the Internet-based shareholder voting application.