

smart**primes** - Advanced Information Security

Company & Product

Vision & Mission

Vision

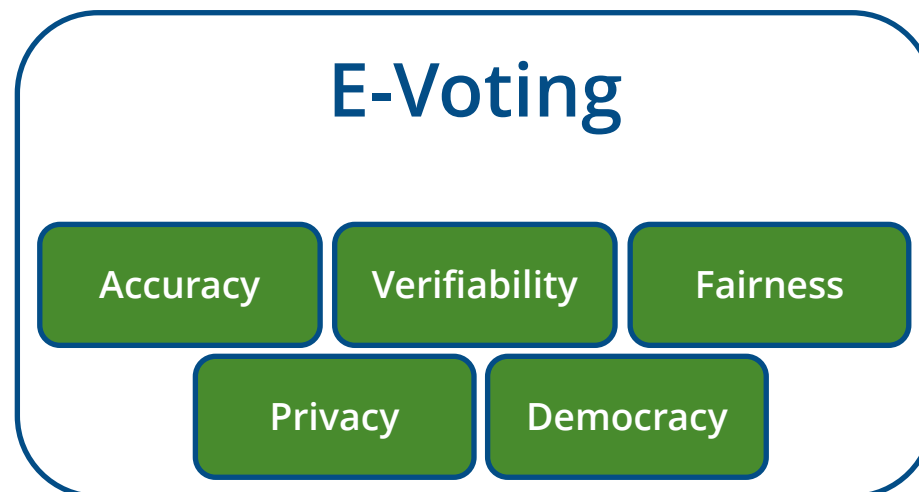
Leading provider of software solutions in crucial areas as e-Voting – information security pushed to a new level!

Mission

By applying modern cryptography we engineer software solutions for secure and verifiable processes.

Requirements for a Voting System

- **Accuracy** – Votes can not be modified (integrity) and not be deleted (completeness).
- **Democracy** – Only eligible people can vote and they can only vote once.
- **Fairness** – No intermediate results can be published.
- **Privacy** – Nobody sees, if and how somebody has voted.
- **Verifiability** – Anybody is able the verify the voting.



Requirements for

Das E-Voting des Bundes ist nicht mehr zeitgemäß

E-Voting to Get Better Trackability and Support

E-Voting in der Kritik Übungsabbruch nach Abstimmungsspanne?

E-Voting to Become More Transparent (1)

Verifiability

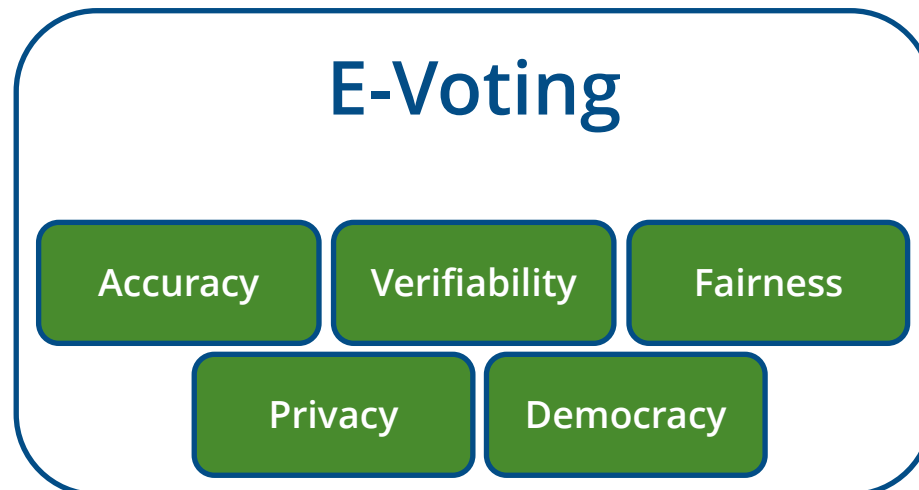
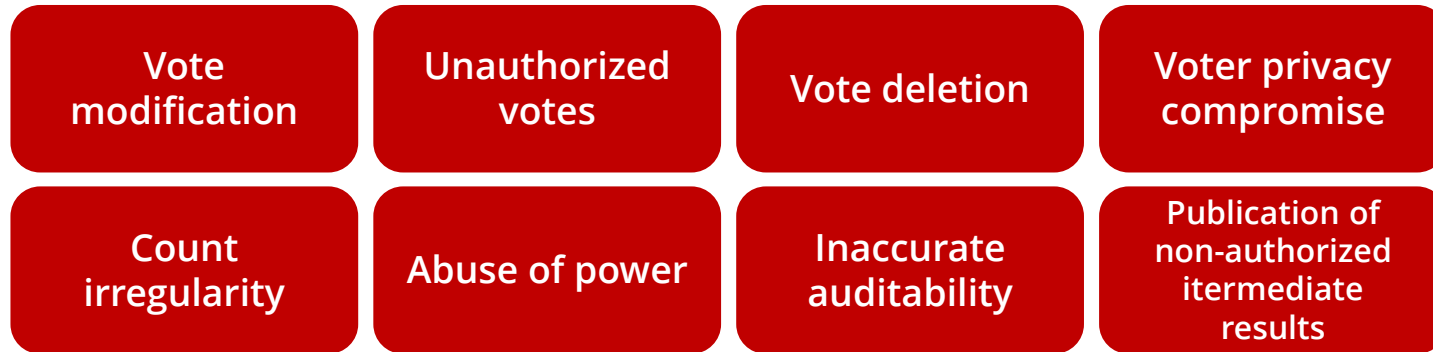
NDP vote dis...
March 29, 2012 - 4:23am BY SELENA

Studie zu verifizierbaren Vote électronique-Systemen
Im Jahr 2011 hat die Bundeskanzlei der Berner Fachhochschule (BFH) der Studie zu verifizierbaren Vote électronique-Systemen zu erarbeiten. Die Studie heute veröffentlicht. Die Vorschläge der BFH, welche aufgrund der Rahmenbedingungen nur längerfristig umgesetzt werden können, werden Weiterentwicklung von Vote électronique einfließen.
Im Februar 2011 hat die Bundeskanzlei der BFH der Entwicklung eines verifizierbaren Vote électronique-System prüfen. Im August 2011 hat das Forschungsteam rund um Haenni der Bundeskanzlei die Studie „Konzept und Implikationen von elektronische-Systemen“ unterbreitet. Nach einer Bundeskanzlei wurde bis Ende Januar 2012 auch noch eine Vernehmlassung des Konzept
Die BFH hat ein umfassendes Konzept für ein sicheres und verifizierbares System vorgelegt. Im Zentrum des Konzepts steht ein kryptographisch auf ausgelegt ist, die kritischen Sicherheitsanforderungen zu gewährleisten und zeitlicher Aufrechterhaltung des Stimmgeheimnisses zu ermöglichen (vgl. S. 2).
Aktiven zur Weiterentwicklung von Vote électronique
Die Schätzung der Bundeskanzlei stellt der Verifizierbarkeit dar. Kurz- bis mittelfristig ist die Umsetzung nicht umgesetzt.

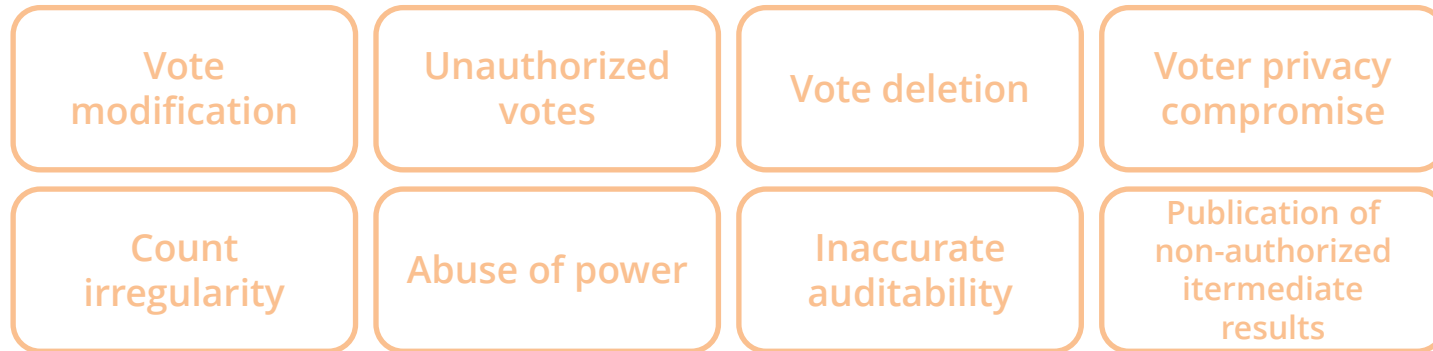
Parliament is looking to amend the electronic voting procedure in such a way as to make it possible for voters to check whether their votes have been registered correctly.
Starting from 2005, e-voting has been used in five elections in Estonia. In order to make the system more transparent, legislators are now



Threats



Solution



primevote

Private, Verifiable Internet Voting

Accuracy

Verifiability

Fairness

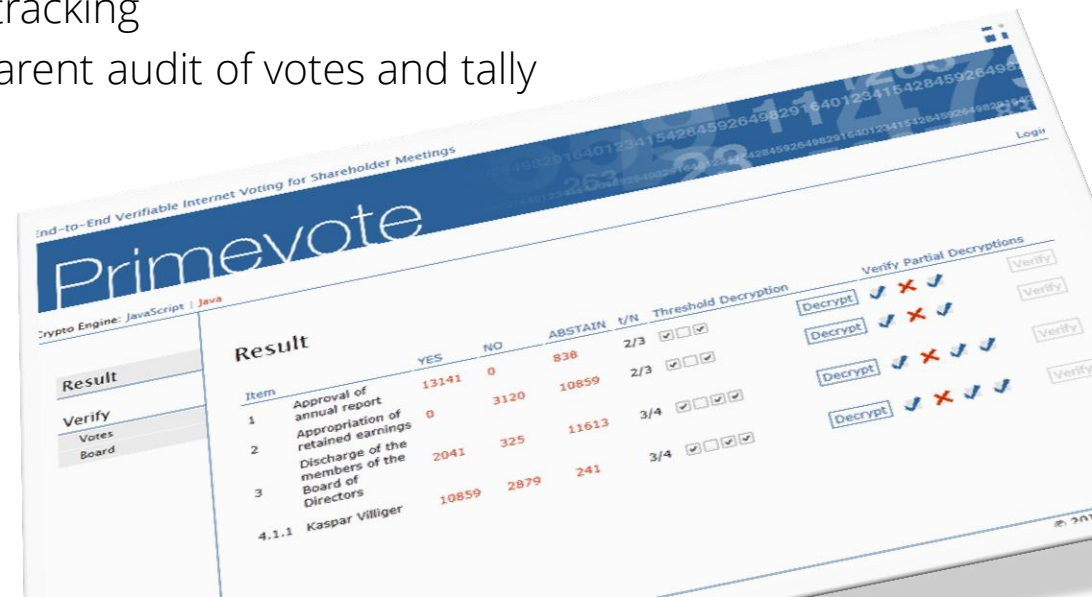
Privacy

Democracy

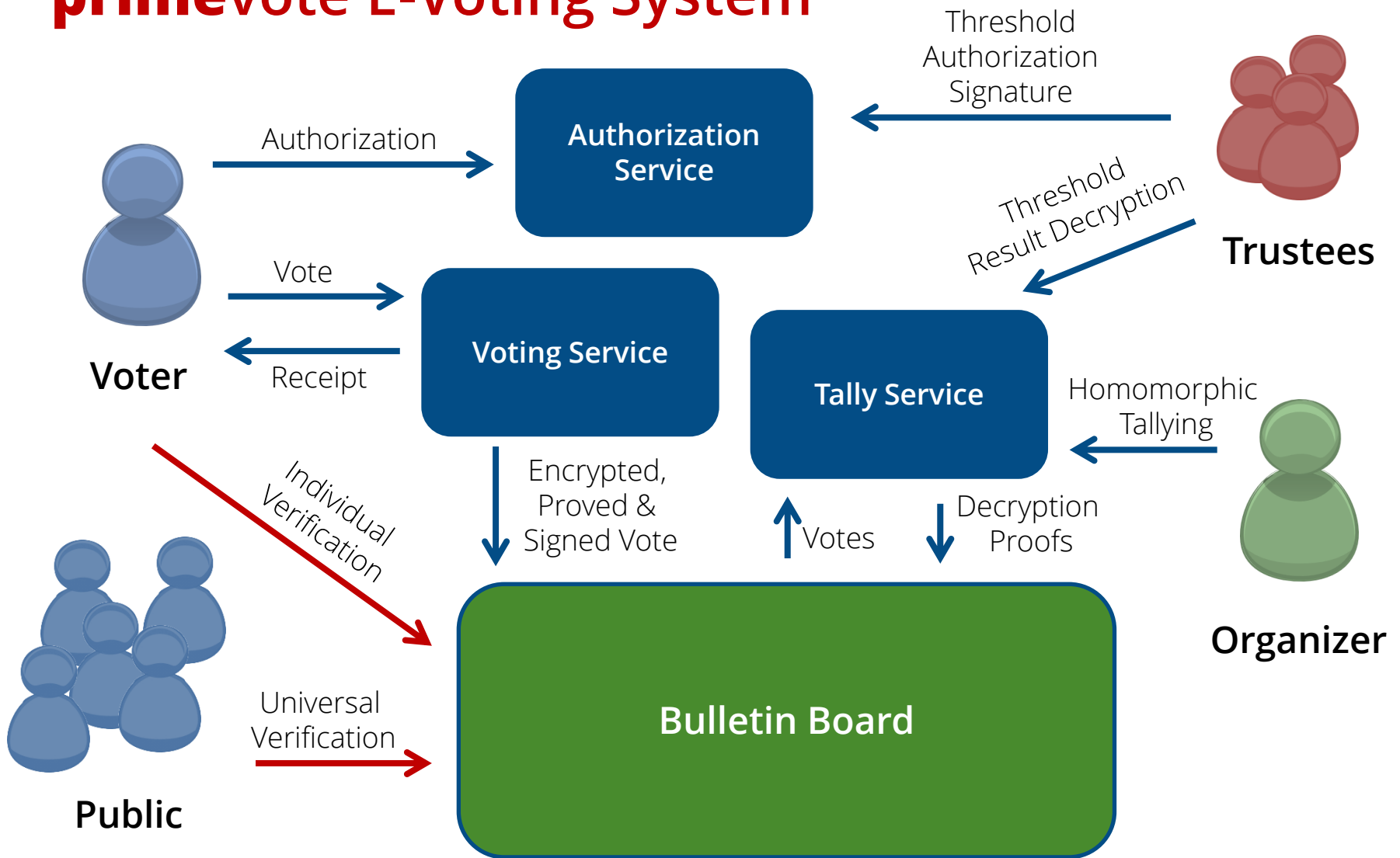
primevote – Private, Verifiable Internet Voting

- Prototype developed during the MSE master thesis by Halm Reusser and Christoph Galliker
- Technology based on modern cryptographic protocols
 - Privacy protection
 - Authority distribution
 - Robust against internal or external manipulation
- **End-to-End Verifiability**
 - Individual verifiability – Ballot tracking
 - Universal verifiability – Transparent audit of votes and tally

Due to the verifiability, people will trust more in **primevote** than postal voting.



primevote E-Voting System



More smart**primes** Business Areas

Crucial Business Areas

E-Health

E-Business

E-Voting

E-Government

E-Cash

Requirements

Democracy

Privacy

Fairness

Accuracy

Verifiability

smart**primes** Technology

Team



Halm Reusser

MSc in Engineering
Co-Founder

CEO

- Finance & Administration
- Human Resources
- Project - & Product Management



Christoph Galliker

MSc in Engineering
Co-Founder

Director

Business Development

- Legal
- Research
- Marketing & Sales



Dani Michel

MSc in Engineering

CTO

Advisory

UAS Rapperswil



Prof. Dr. Andreas Steffen
Dipl. El. Ing. ETH
Head of Institute for
Internet Security

CTI Start-up Coaching



Hans Oury
Dipl. El. Ing. FH
MAS Corporate Finance

E-Voting Competence Center



Prof. Dr. Eric Dubuis
Dr. sc. techn. ETHZ
Vice President

smart**primes**

