University of Fribourg

Bern University of Applied Sciences

Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting

Oliver Spycher

Tallinn, September 29th, 2011

Outline

Measures for Trust Establishment

Outline of the Norwegian System

The Measures in the Norwegian System

Outline

Measures for Trust Establishment

Outline of the Norwegian System

The Measures in the Norwegian System

Some Desirable Properties

- **Correctness**: The published result reflects the electorate's intensions correctly
  - → one-voter-one-vote, only eligible voters
  - → no stuffing, deletion, altering
  - → reliable tallying
  - → no pressure
- **Secrecy of the ballot**
- **Fairness**: No premature results obtainable
- **Receipt-freeness / coercion-resistance**: no advantage for proving how one voted

Some Problems Specific to Internet Voting

- **Scalability of attacks**
- **Trust towards operator, vendor**
- **Sound authentication**
- **Insecure computers, insecure Internet**

Security and Trust

- **We tend to assume strong threats, including operators**
  - → Who try to manipulate the result
  - → Break secrecy
  - → Coerce voters and buy votes
- Researchers *cannot* judge whether a system is sufficiently secure
- But they *can* assess whether a system holds specific features
- **Measures to establish trust** should aid at bridging the communication gap between policy makers / public and experts from research
- Security mechnisms are merely a precondition to trust

Our contribution

Find a set of measures applied in Norwegian System

- separation of duty, verifiability, vote updating
- test elections, third party clients
- foundation: transparency, evaluation

(This list should be extended)

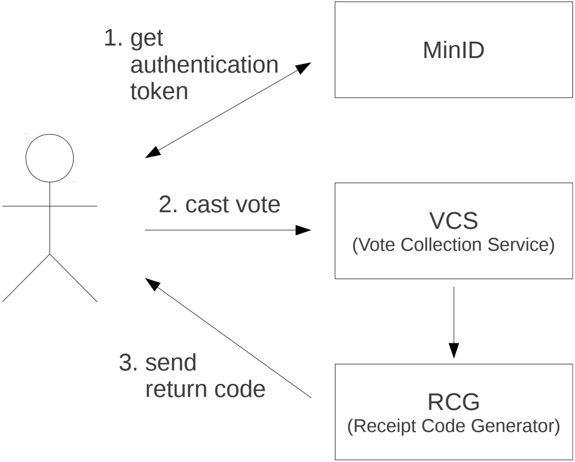
Outline

Measures for Trust Establishment

Outline of the Norwegian System

The Measures in the Norwegian System

Brief Outline / Voting


1. get authentication token

MinID

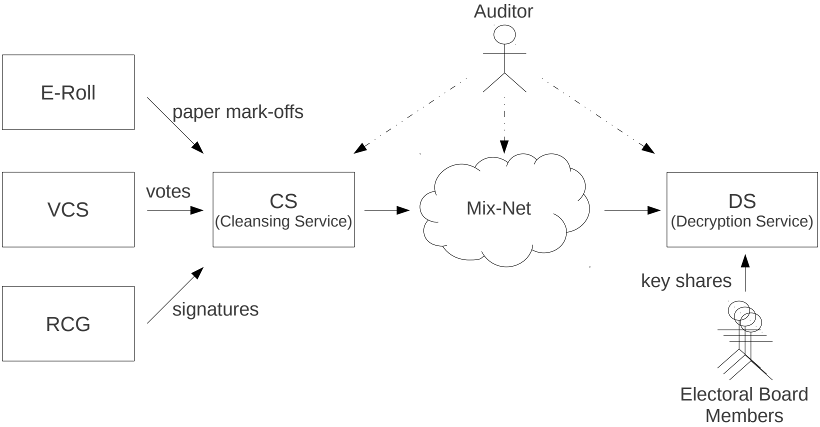
2. cast vote

VCS
(Vote Collection Service)

3. send return code

RCG
(Receipt Code Generator)

Brief Outline / Tallying



Outline

Measures for Trust Establishment

Outline of the Norwegian System

The Measures in the Norwegian System

Separation of Duty

Separate secrecy-critical information and integrity-critical power among multiple entities

Implications

- No need to trust one single entity (person / computer, site, vendor)
- Trust only in 1 out of many at being reliable and independent

Need to expose payoff and limitations!

Separation of Duty for Secrecy

Conclusions

- Client learns vote, argumentation of re-voting
- VCS and RCG can break secrecy, buy votes
  - → VCS and RCG operated by different organizations, locations. Same vendor
- DCS and any of VCS, RCG, CS, Auditor as well
  - → DCS and CS same location, same vendor
  - → Auditor different vendor. Trade-off in secrecy and integrity over number of auditors
- 6 EB members and any of VCS, RCG, CS, Auditor as well
- Each node of the mix-net operated by same person, same location, same vendor

Verifiability

Allow voters to verify the correctness of the published result

- cast-as-intended
- recorded-as-cast
- eligibility
- universal

Implications

- No need to trust any entity (computer / person, site, vendor)
- Verifiability vs. lacking proofs (research ongoing)

Need to expose payoff and limitations!

Verifiability

Conclusions

- Cast-as-intended, given
  - → Computer and SMS-receiver do not collude
- Recorded-as-cast, given
  - → MinID trustworthy and
  - → Computer and RCG do not collude and
  - → VCS and RCG do not collude
- Reason: No proofs forwardable to parties external to the system
- Universal and eligibility, given at least 1 honest auditor
- Otherwise, auditor and one out of CS, DCS, 1 mix-node can break integrity

Vote Updating

Allow voters to update by i-vote and / or paper vote

Implications

- Side-step vote selling, confusion
- Trust that cast votes reflect free will
- Sound authentication required

Conclusions

- Implemented
- Protection from vote-buying only regarding outside players

Transparency

Open documents for experts to assess and evaluate:

- Technical requirements, including security concept
- Technical implementation, source code, cryptographic protocol
- Exposition of remaining risks
- Assessment of simplified documentation for average voters

Assessment of simplified documentation to achieve credibility among policy-makers / public

Conclusions

- Project follows a transparency guideline
- Implemented or plan to implement propositions from our side
- Implements many of the measures to some degree
- However constraints are not always made explicit
- Example: Constraint regarding cast-as-intended not pointed out
- Example: Power of MinID contradicts the spirit of separating VCS and RCG
- Dynamic project, information easily outdates

Thank You!

Questions / Remarks

e-voting.bfh.ch and **www.secuso.cased.de**

contacts, papers, reports