E-Voting and Implementation

Sven Heiberg, Smartmatic-Cybernetica CEIV

SMARTMATIC CYBERNETICA

Providing Technology for Elections

- Cybernetica AS
  - Established in 1997, roots in Academia since 1960
  - Architects of the e-Estonia ecosystem
  - R&D of Estonian i-voting system since 2003

- Smartmatic
  - Modernizing elections globally since 2000
  - Diverse online voting projects:
    - Pilot projects: Mexico, Benin
    - Organizational elections: Estonia, Germany
    - Municipal elections: Norway, Canada, Australia
    - Governmental elections: ongoing RFI/RFP processes

Estonian Experience

- 14th consecutive election using online voting
  - Established legal framework supporting online voting
  - Advanced technological infrastructure for citizen-government communication
  - Comprehensive understanding of online voting risks
  - Awareness of differences between paper and electronic voting
  - Robust organizational support for online voting technologies
  - Modern, reliable and secure technology
  - Multiple opportunities to learn from past mistakes

- Steady interest in the Estonian experience
- Similar challenges in new opportunities

Legal Framework

- **Anti-Coercion Mechanisms vs. Electoral Law**
  - In Estonia, voters can vote online multiple times; only the last vote counts
  - Paper vote takes precedence over electronic vote
  - Supreme Court discussion in 2005

- **Ballot Presentation**
  - Paper ballot designs often have detailed regulations
  - These designs may not suit digital screens (PCs/smartphones)
  - Technology can assist users by:
    - Warning about malformed ballots
    - Providing search capabilities

Voter Eligibility Verification

- Estonia – widespread use of PKI based ID-cards, mID, and Smart-ID
  - Digital signature is legislated and widely used
  - Online voting turnout in 2005: 1.9%
- Digital signature: a core pillar of security
  - Ensuring eligibility, integrity, and non-repudiation
- Online-voting can boost the use of eID in the country
- Alternatives either unusuitable for governmental elections or increase the cost of a single election
  - OpenID Connect
  - Election specific credential generation and distribution

Risk-based Selection of Technology

- **Initial Risk Analysis for Estonian Online Voting (2003):**
  - “The weak point of the scheme, is the need to trust central servers and computers of the voters. Is such a compromise reasonable? In our opinion – yes." (Ansper et al., 2003)”
  - Vulnerabilities exist, countermeasures also exist, residual risk is accepted
    - Secure concept: authentication, ballot secrecy, integrity
    - Security engineering: system architecture, implementation, deployment
    - Organization: documented auditable procedure developed according to risk analysis, definition of organizational roles
- The initial risk analysis is obsolete today
- **Current Goal:** No trust in central servers or voters' computers

Trust in Voters' Computers

- Individual verifiability
  - Voter has means to verify some of the following claims
    - Cast-as-intended
    - Accepted-as-cast
    - Tallied-as-recorded

- Individual verifiability may affect coercion
- How to act on failed verifications?

Trust in Central Servers

- Universal verifiability
  - Observer (third-party data auditor) can directly verify:
    - Only votes by eligible voters are in the ballo box
    - At most one vote per voter is in the ballot box
    - No un-authorized modifications to the ballot box have occurred
    - The result is calculated correctly

- Universal verifiability contradicts ballot secrecy unless carried out in a privacy-preserving manner.
- Modern cryptographic mechanisms for online voting protocols (homomorphic encryption, mixnets, zero-knowledge proofs) are often not standardized in e.g. FIPS or Common Criteria.

Organizational Structure

- Reliable, transparent and privacy-preserving online voting requires co-operation of several organisations
  - ESEO – election organizer
  - RIA – vote collection, election management platform
  - Population registry – eligibility provider
  - PPA – PKI
  - SK – ledger service, CA, OCSP, TSA
  - NEC – participation in private key management
  - Auditors – observing procedure and data
  - Cybernetica – support for software

Security Considerations

- **Careful Distribution of Duties**
  - Ensures security across organizational boundaries in high-risk environments.
  - Key assumption in using modern security protocols: ledger, threshold decryption, mixnets
- **Election-as-a-Service Model**
  - Viable option for lower-risk elections, offering comprehensive solutions from specialized vendors
- **Platform ownership / co-development**
  - Allows fine grained control over features to fit into specific environment

Towards Online Voting

- Several challenges exist before implementation
- Unlikely to find a perfect off-the-shelf solution
- Best practices exist; involve specialists rather than reinventing the wheel
- Allow time for concept development, consider piloting

Thank you! Questions?

Sven Heiberg – sven.heiberg@ivotingcentre.ee

https://cyber.ee/
info@cyber.ee
cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica

SMARTMATIC CYBERNETICA