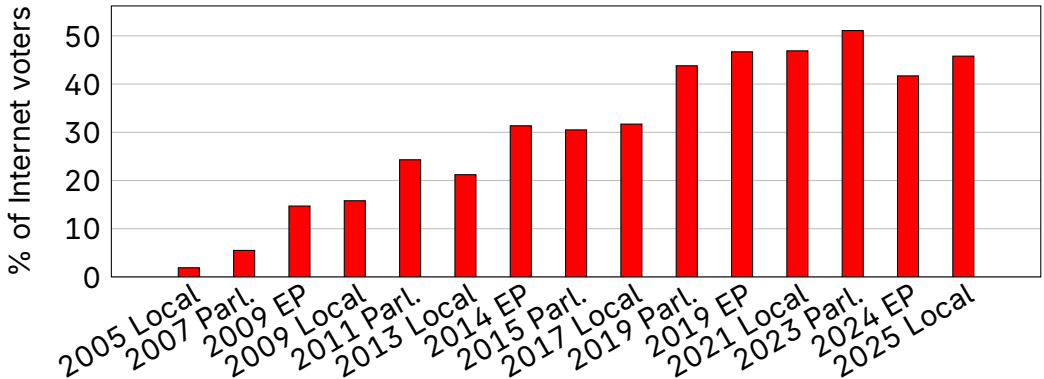
Internet voting in Estonia – past, present and future

Jan Willemson
janwil@cyber.ee

Estonian Internet voting timeline



Political and societal context

- In late 1990s and early 2000s, Estonia had had success with several IT-related endeavors:
  - X-Road data access middleware,
  - ID-card (and a bit later mobile ID), together with the Digital Signature Act,
  - Tiger Leap programme for schools,
  - Look At The World educational programme for senior citizens,
  - E-banking and tax declarations.

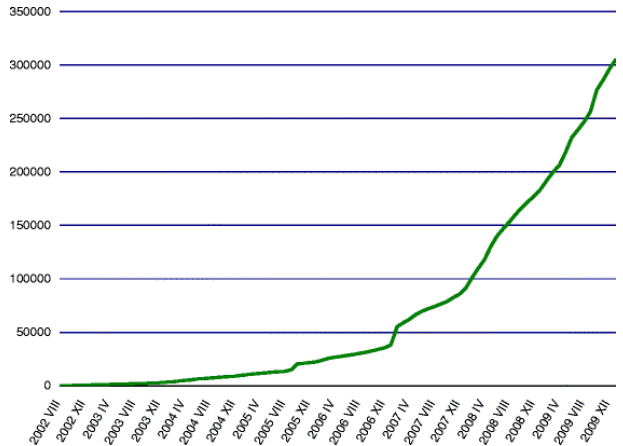
Political and societal context

- In late 1990s and early 2000s, Estonia had had success with several IT-related endeavors:
  - X-Road data access middleware,
  - ID-card (and a bit later mobile ID), together with the Digital Signature Act,
  - Tiger Leap programme for schools,
  - Look At The World educational programme for senior citizens,
  - E-banking and tax declarations.
- As a result, it was easy to find political consensus in introducing Internet voting.

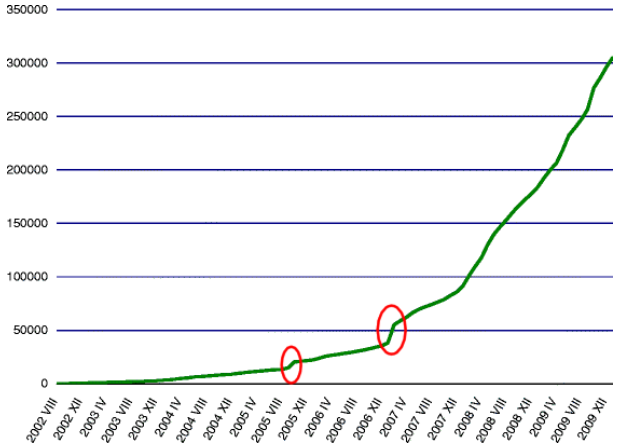
ID-card: 2002 – ...

- The only *compulsory* ID
- Travel document
- Equipped with two cryptographic public/private key pairs
  - One for authentication, one for digital signing
  - First RSA1024, then RSA2048 and now ECC P-384
  - Digital signature *legally equivalent* to a hand-written one

Issued ID-cards 2002...2009



Issued ID-cards 2002...2009



Opposition to Internet voting

- Soon, some of the parties started fearing that they may lose seats because of Internet voting.
- So, they started opposing to it. References to security issues have been a standard part of the narrative.
- There has always been one major I-voting opposing party, but this party has surprisingly changed over time.
  - Koonderakond
  - Keskerakond
  - EKRE

https://delfi.ee/

2011 Parliamentary elections

- A history student created a proof-of-concept malware capable of blocking or manipulating votes on users' computers.
- An elderly lady voting for more than 500 times.
- The first invalid vote occurs.
- As aftermath to 2011 elections, individual verifiability was added.

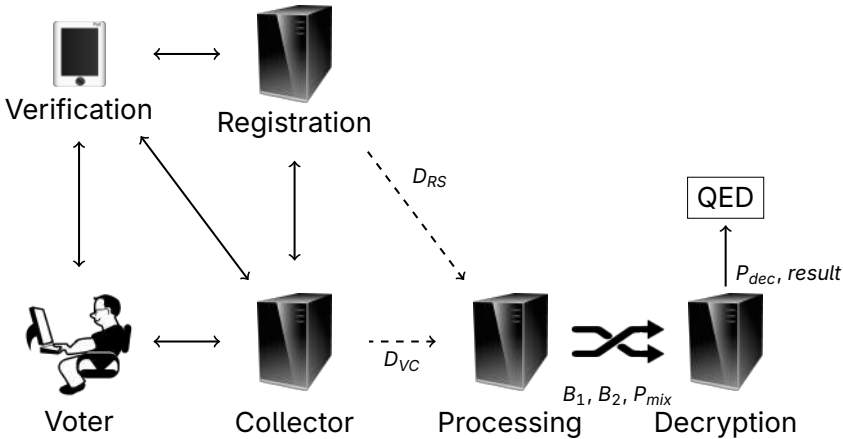
Image source: `https://www.ohtuleht.ee/`

2014 elections

- 3 days before elections, Alex Halderman & Co appeared in Tallinn, presenting their report on the Estonian system and demanding i-voting to stop immediately.
- As aftermath, a new protocol suite IVXV was introduced in 2017.

https://estoniaevoting.org/

IVXV 2017–2025



IVXV and cryptography

- Votes are encrypted using ElGamal cryptosystem on the P-384 elliptic curve.
- The votes are signed using ID-card, mobile-ID or SmartID.
- Zero-knowledge proof of correct mixing.
- Zero-knowledge proof of correct decryption.
- In 2027, zero-knowledge proofs of ballot correctness will be added.

IVXV and cryptography

- Votes are encrypted using ElGamal cryptosystem on the P-384 elliptic curve.
- The votes are signed using ID-card, mobile-ID or SmartID.
- Zero-knowledge proof of correct mixing.
- Zero-knowledge proof of correct decryption.
- In 2027, zero-knowledge proofs of ballot correctness will be added.
- What about the quantum threat?
  - The eID will have to transition anyway.
  - For vote secrecy, post-quantum encryption is needed.
  - The latter is tricky, because we want the ZK proofs to work.
  - See also the recent Estonian Post-Quantum transition roadmap.

Why can’t we vote on mobile phones?

- They are just computers, right?

Why can’t we vote on mobile phones?

- They are just computers, right?
- Wrong.
  - Mobile ecosystems are much more closed.
  - Application integrity is much harder to verify independently of the vendor.
  - Small screens force undesirable trade-offs.

Why can’t we vote on mobile phones?

- They are just computers, right?
- Wrong.
  - Mobile ecosystems are much more closed.
  - Application integrity is much harder to verify independently of the vendor.
  - Small screens force undesirable trade-offs.
- Estonian legislation has recently been updated to allow mobile voting.
- Mobile voting software was also created and tested.
- However, 2025 local elections did not yet use this option, and 2027 parliamentary elections will not either.

Remote identification is hard

- eID performs digital *authentication*.
- But this only means that at the other end of the communication there is a specific cryptographic key, not a person.
- There have been rumors about ID-cards being misused for e-voting in elderly care homes.
  - No cases have been proven, though.

Is biometry an answer?

- In principle, facial biometry could be used as a second factor.
  - In a polling station, your face is examined afterall.
- The technology has only recently matured enough to be reliable "in the wild".
- Facial recognition would actually work better with mobile device cameras, so this could support mobile voting.

Image source: `https://bi.com/`

Thanks!

- This work was supported by
  - CHESS – The Cyber-security Excellence Hub in Estonia and South Moravia,
  - QARC – Quantum-Resistant Cryptography in Practice, and
  - the Estonian Research Council grant (PRG2177).

- I will be happy to answer any questions.
- Drop me an email: `janwil@cyber.ee`

©2026 Cybernetica AS