



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

E-State and Proactive Risk Management

Kaur Virunurm, Head of R&D

Liisa Past, CRO

Estonian Ecosystem

- 400 m digital signatures given
- 95% of taxes declared online
- 1 in 50 medical prescriptions on paper
- 1/3 of votes cast online

The Foundation: Secure Digital ID



Additional eID tokens

Mobile-ID: SIM-card-based token

Digi-ID: additional card for digital use only

E-Residency card

Diplo-ID



eIDAS

EU regulation on electronic ID-s & signatures

<https://en.wikipedia.org/wiki/EIDAS>

Creates mutual trust by setting rules on:

- technology
- processes
- organisations

Establishes four levels of trust

- from „snake oil“ to „certified hardware“ (QSCD)

ID-card and mID are on the highest level

Use case: I-voting

- Another method of early voting since 2005
- Votes cast online
- Relies on ecosystem (identity, pop registry)
- Plateaued at 1/3 of votes
- No (dis)advantage to any demographic or party
- Secure, no significant incidents so far
- Fulfills constitutional and security criteria for elections

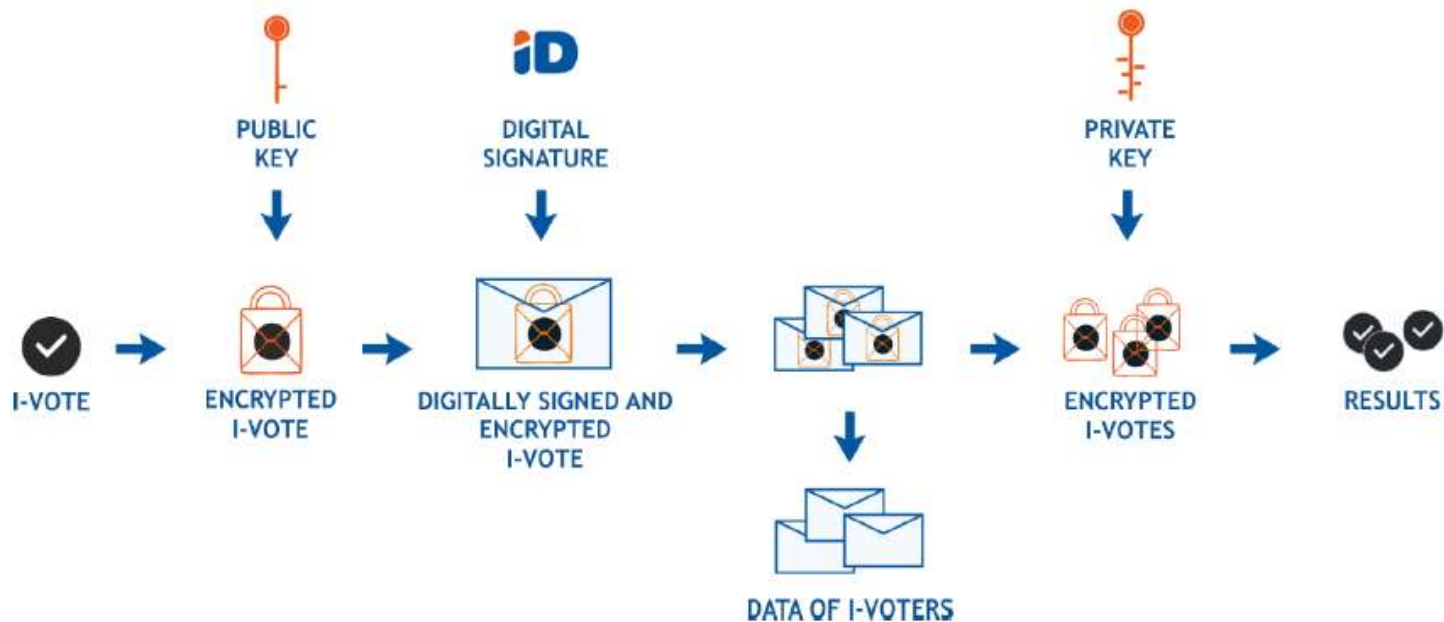
Open and Government-Owned

- No legacy or proprietary solutions
- Open by law
- Open specifications, protocols, documentation
- Open procedures, public observers
- Open source code

References

- www.valimised.ee – EN – e-voting – documentation
- <https://github.com/vvk-ehk/ivxv> - real source code

Estonian I-voting - technology



Double envelope scheme

Digital „copy“ of real-life remote voting procedure

Unsigned votes are sealed and placed into a signed envelope

Signed envelopes are discarded after verification

Uses PKI (asymmetric crypto) extensively



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Holistic and comprehensive risk management

Well beyond technical solutions

Hybrid threats, inc. communication



SHARE



SHARE
46



TWEET



COMMENT



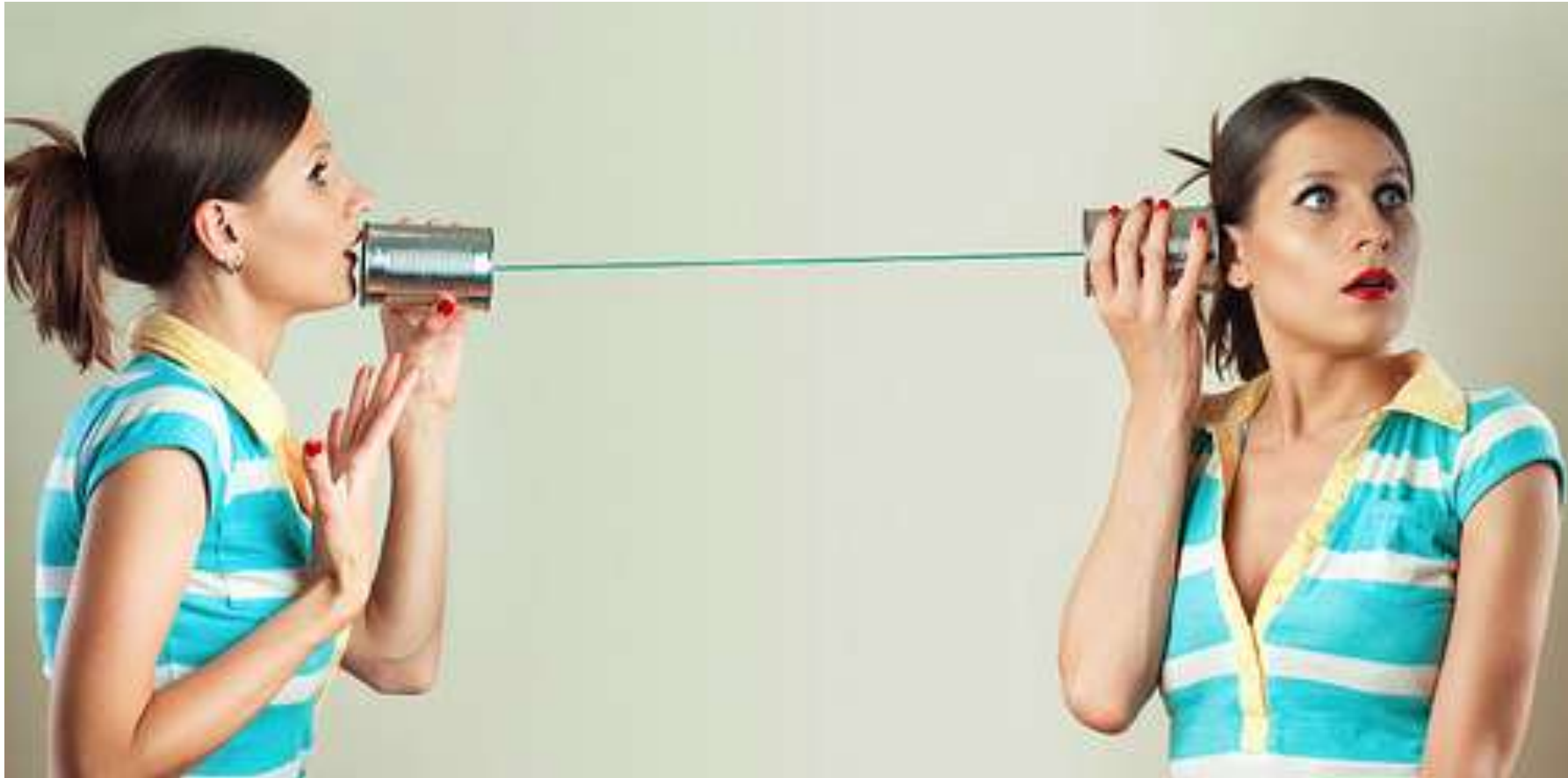
EMAIL

HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE



Defense minister Jaak Aaviksoo got help from NATO in the wake of the cyberattacks. *

Management and stakeholderism



One unique live dependency



ID-card firmware flaw

- Cause

- Firmware error in chip cards
- Keys are weak, breaking them requires less resources than it should
- Nothing broken yet, just a theory / vulnerability
- Not an incident
- Cards (and everything on them) is certified

- Solution

- Update card software and create new keys
- Remote
- Will happen after elections

Agressively open risk management

- Impact: 750 000 cards (55%)
- Only way to ensure credibility, cooperation
- Avoided tsunami of crisis communication
- United front to critics
- Allowed to focus on solution



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

No 100% security 100% of time

Liisa Past, liisa.past@ria.ee

Kaur Virunurm, kaur.virunurm@ria.ee