



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Estonian ID-card - public risk management

Taimar Peterkop
Director General

History

- 7 October 2002 – first digitally signed document
- I-voting since 2005
- 1 January 2016 – the Information System Authority became responsible for eID
- 1 July 2017 – new Emergency Act (authentications and digital signatures became vital services)

Numbers

- Over a billion operations over the past 15 years (428 million digital signatures and 611 million authentications)
- 1,3 million valid ID-cards
- 350 000 cards in everyday use
- 5000 e-services
- The discovered security risk affected 800,000 cards (cards issued as of 16 October 2014)

Nature of the security risk

The private key can be computed from the public key, which means that:

- it is possible to digitally sign a document in the name of another person
- it is possible to enter e-services in the name of another person
- it is possible to steal a digital identity without having the physical card
- decrypt documents encrypted with the ID card

Countermeasures

- Making a potential attack more difficult – closing the public key database (5 September 2017)
- Additional security measures in e-services
- Alternative –use of mobile-ID
- Deploying other type of cryptography (elliptical curves) and providing the possibility to update ID-cards remotely
- Suspending the certificates of ID-cards with a security risk
- Public risk management, because e-Estonia is based on trust

Current situation

- Vulnerability has not been exploited
- 95 % users updated their ID-cards (500 000 cards)
- Alternatives have become more popular – 160 000 mobile-ID users
- Most of the e-services support the updated cards
- Active use of e-services (people use the services as actively as before)
 - 304 000 not updated certificates were revoked in the end of March

Further steps

- The 'lessons learned' has been completed
- Ecosystem view, awareness, preparedness and management
 - Which competencies are indispensable in the state; with which should we rely on others; and what are we developing with others?
 - Who are our customers and how can we reach them?
- New ID-card procurement (the ID-cards of the new manufacturer will be issued as of September 2018)



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Thank you!