TALLINN UNIVERSITY OF TECHNOLOGY
CENTRE FOR DIGITAL FORENSICS AND CYBER SECURITY

Lessons we learned: the Estonian view

Rain Ottis, PhD

Team

In alphabetical order:

- Ahto Buldas
- Martha Jung
- Kaja Kuivjõgi
- Anna-Maria Osula
- Rain Ottis
- Jaan Priisalu
- Liisa Tallinn
- Toomas Vaks

Timeline

- AUG 2017 – EISA notified of the problem
- SEP-NOV 2017 – developing and deploying the fix
- MAR 2017 – remaining certificates revoked

- FEB-APR 2018 – interviews & research
- 16 APR 2018 – FOUO version submitted
- 09 MAY 2018 – Lessons learned conference

General observations

- Global event with a special use case in Estonia
  - Multiple national IDs, TPM, etc.
- Well handled, all things considered
  - eGov did not break (much)
  - trust remains high
- Situational awareness
  - Threat picture changes over time
  - Problem and solutions become more tangible over time

Lessons identified

- *Quo vadis*, eID?
- ID Card is more important than we know
  - What else is important?
  - How to map cross-dependencies of critical services?
  - How to escalate risk (assessments) to management?
- Early warning system failed

Lessons identified

- How to handle a **non-incident**?
  - theoretical vulnerability
  - no damage
  - no exploits in the wild
  - potential effects may be severe

Lessons identified

- Proactive communication stance worked.
  - However, technical communication could have been better in the beginning
- Limited pool of experts
  - Duplicate, if possible
  - Engage and cultivate the community
  - International arrangements

Lessons identified

- Redundancy helps
  - ID card + Mobile ID
  - RSA + elliptic curve
  - PPA office + remote renewal
- This will not be the last such event
  - Post-quantum solution sought
  - Concept of identity is changing
  - Nobody wants to go back to paper, even if they could

Additional reading

Buldas, A., Jung, M., Kuivjõgi, K., Osula, A.M., Ottis, R., Priisalu, J., Tallinn, L., Vaks, T. ID-kaardi kaasuse õppetunnid. Tallinn University of Technology, 2018.

Cybernetica Case Study: Solving the Estonian ID-card Case
https://cyber.ee/en/news/cybernetica-case-study-solving-the-estonian-id-card-case/

Nemec, M., Sys, M., Svenda, P., Klinec, D., Matyas, V. The return of Coppersmith's attack: practical factorization of widely used RSA moduli. In the ACM SIGSAC Conference on Computer and Communications, CCS'17, pp. 1631—1648, 2017.

Thank you!