Estonian eID Security: Open Issues

Arnis Paršovs

November 7, 2013

STACC Software Technology and Applications Competence Center

European Union
Regional Development Fund

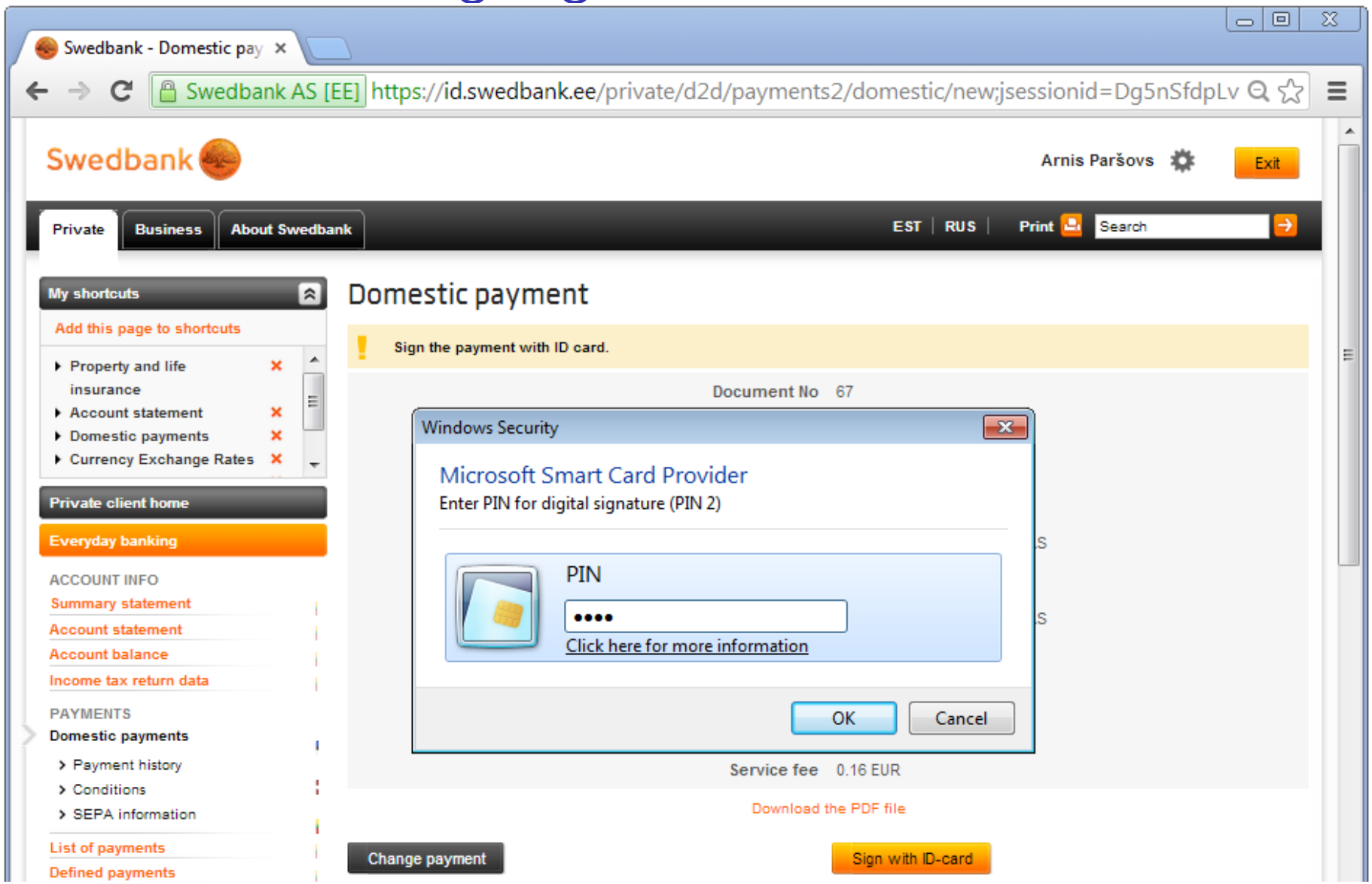
Investing in your future

ID-card Authentication

Arnis Parsovs.
Practical Issues with TLS Client Certificate Authentication.
Cryptology ePrint Archive, Report 2013/538, 2013.
http://eprint.iacr.org/2013/538.pdf.

- What are the practical issues concerning deploying TLS CCA?
- Measurement study of 87 Estonian service providers
- TLS CCA solves the authentication problem on the Internet
- Server and browser implementations could be improved
  - Where to get resources for that?

Signing in the Browser



What is being signed?

What if this is not a connection to Swedbank's server?

Mobile-ID

- Legally equivalent to the ID-card
- More convenient than the ID-card
- Less secure than the ID-card:
  - Anyone can initiate the protocol
  - Not bound to TLS channel
  - Non-visibility of what is being signed
- New trust assumptions:
  - Service provider
  - DigiDocService provider
  - Mobile operator
- Mobile-ID to take over ID-cards?
- Moving to signing in the cloud?

ID-card Software Security

ERR | News
Estonian Public Broadcasting

After Bug Fix, Some Fear Thousands May Not Update Digital Signing Software

Published: 28.08.2013 12:02

The national ID card software website, which gives access to Estonian electronic services such as digital signing, said on August 22 that a critical security vulnerability had been fixed and that a new software update is available.

"A critical error has been fixed in the processing of DDOC files. Exploiting this error could have rendered it possible to overwrite random files in the user rights of the victim's computer, if the attacker were to lure the user in to opening specially formatted digital signature files," said the software downloading website.

`http://news.err.ee/sci-tech/4d7848c6-1e09-454b-a9f3-6a422970c16f`

- From fake signatures to arbitrary code execution
  `https://svn.eesti.ee/projektid/idkaart_public/trunk/libdigidoc/RELEASE-NOTES.txt`
- ID-card software should be a part of Estonian CII
  - Perhaps along with Internet voting software
- How to involve more world class security researchers?
- Vulnerability rewards programs
  - Monetary reward and being credited on a "wall of fame"
  - More cost efficient than hiring full-time security researchers

Matthew Finifter, Devdatta Akhawe, and David Wagner.
An Empirical Study of Vulnerability Rewards Programs.
In *Proceedings of the ACM Conference on Computer and Communications Security*, Washington, DC, August 2013.

Encryption

Postimees IN ENGLISH

NEWS | НА РУССКОМ | EESTI KEELES | E24 | SPORT | ILM | NAINE24 | ELU24

Local News | Economy | Sport | Opinion | Culture | Newspapers overview | Estonian ma

LOC

Publishe

Ilve
indi

Toomas Hendrik Ilves.
Foto: AFP/Scanpix

To the knowledge of President Toomas Hendrik Ilves, Estonia's special security services have not been in cooperation with America's NSA to make use of its PRISM programme total surveillance data.

Is Edward Snowden, the man who leaked confidential documents regarding the US total surveillance, a whistle-blower doing a service to the societies of USA and the West, or a traitor in the order of Herman Simm?

"We might take a look at what we have got: we are the only country in Europe enabling use of ID cards to send encrypted e-mails."

- Few problems:
  - Usability issue
  - 1024-bit keys
  - Private key copies

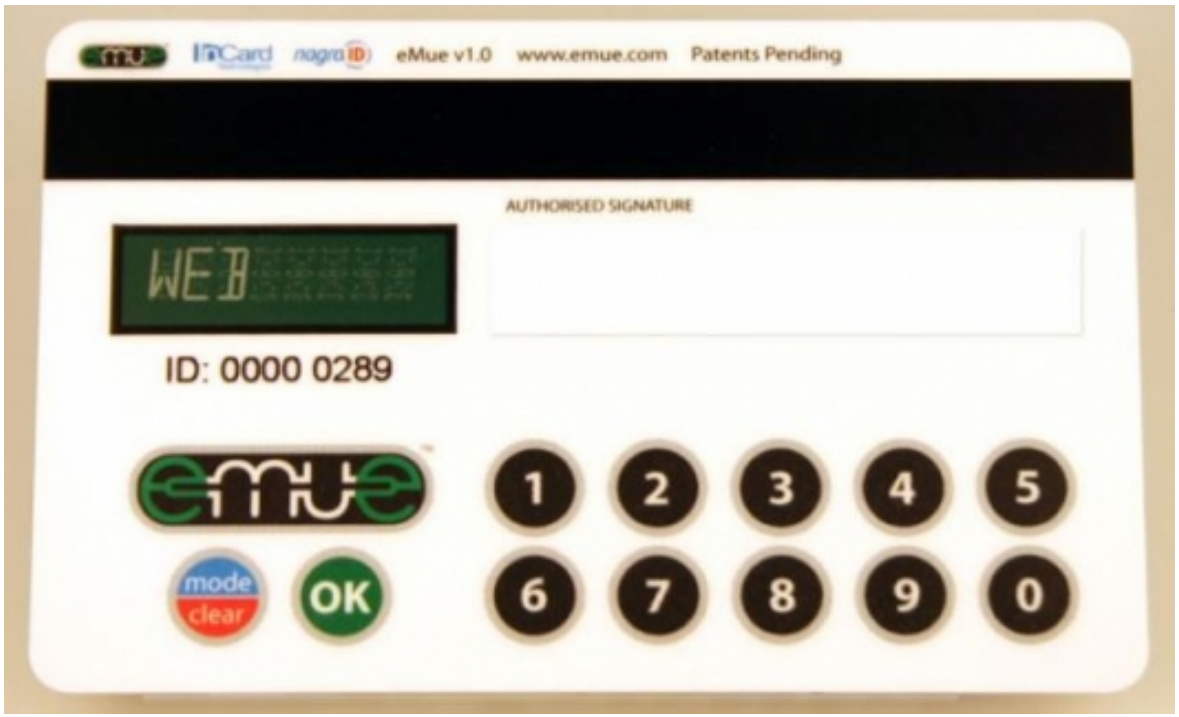
http://news.postimees.ee/1297268/ilves-wishes-europe-would-ease-its-indignation-a-bit

Physical Access

- Installation specific physical access tokens
- Why ID-cards are not used as unified access tokens?
  - No contactless interface
  - Personal data file not protected
  - Trust your PIN to a terminal?
  - Sign unknown data?

Computer Security

- Computers might be the weakest link
- Pinpad readers do not solve the problem
- Could we do better with next-generation smart cards?



Legal Uncertainty

Digital Signatures Act:
§ 3. Legal consequences of using digital signatures
(1) A digital signature has the same legal consequences as a hand-written signature (..)
(3) The giving of a digital signature does not have the consequences provided in (1) if it is *proved that the private key was used for giving the signature without the consent* of the holder of the certificate.
(5) In the cases specified in subsection (3) of this section, the certificate *holder shall compensate for damage* caused to another person who erroneously presumed that the signature was given by the certificate holder, if the private key was used without the consent of the certificate holder *due to the intent or gross negligence* of the certificate holder.

`http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30081K6&keel=en`

- How would this apply in a case of compromised computer?
  a. It is gross negligence – compensate the damage
     - Risk is too high – revoke your certificates
  b. Easy repudiation by having malware in your computer
     - Digital signature is useless – supporting evidence required

Security has to be improved so that only physical attacks remain feasible

Thank you!

Questions, comments, opinions?

arnis@ut.ee