SK Aastakonverents 2014

Uue põlvkonna eID kiipkaart
New Generation of eID Smartcard

“Developments on the EstEID Smartcard Application”

06.11.2014
EstEID Chip Application – Today

- Version 3.5 on ID cards since Monday 20. October
- Change from v3.4 to v3.5 together with new chip platform
- > 1. December – DigiID / e-Residency DigiID with v3.5 and new chip
- ~January 2015 – RP with v3.5 and new chip => Change completed!

- Version 3.5 – redesigned, streamlined, increased security
- New chip: SLE78 with TrustedLogic Java futureproof platform
  - unrestricted support of next generation cryptography
  - support of OAEP => possibility to use PKCS#1 v2.2
  - higher performance
EstEID Chip Application – Development since 2002

- 2001 – copy of FinEID => EstEID v1, 1k certificates, OS: Micardo Public
- 2008 – EstEID v1.1 (2), 1k certificates, no T=1, OS: Multos
  issued as DigiID only starting from May 2010
- 2010 – EstEID v3.0, 2k certificates, OS: Java
  issued January – December 2011
- 2011 – EstEID v3.4, 2k certificates, OS: Java
  a.o. immunisation against PIN/PUK blocking by PIV driver
  issued since January 2012 and replaces v3.0
- NOW – EstEID v3.5, 2k certificates, OS: Java
EstEID with NFC – Why at all

- Reputation: EstEID to be recognised as innovative
  [Link](http://www.ega.ee/files/ID-1%20formaadis%20dokumentide%20funktionaalsuse%20uuring_v2.pdf)
- Explore new application fields
- Consider changed user habits:
  - widespread and growing use of tablet computers
  - tablets rather unsuitable for MobileID: Missing GSM, Impersonal
- Having the opportunity: DigiID as technical playground
EstEID with NFC – What and Where

**WHAT**

- NFC to substitute card reader – Only Computer & Card
- Use of EstEID webservice as of today – choose “ID-card” for login/signing => Avoiding changes on Host side application!

**WHERE**

- EstEID NFC pilot runs on Android devices
- EstEID NFC pilot runs with Google Chrome browser
- EstEID NFC pilot runs with on new DigiID’s
- Phase 1: Selected Beta test pilot group – special permission of PPA
- Phase 2: Enlarged pilot group – special permission of PPA
EstEID with NFC – How it works #1
EstEID with NFC – How it works #2

- Webservice server requests client validation
- Browser (Chrome) provides API to communicate with built-in Android NFC service that integrates to CA (SK)
- User needs to select certificate and validate PIN
- User certificate gets validated against SK’s OCSP (DigiDocService)
- Android service sends back signed client certificate to Browser
- Server validates client certificate against SK’s OCSP
- Secure SSL connection between client and server is set up

... And you are IN

Similar for digital signing
EstEID with NFC – Security Considerations

- No decryption feature in NFC mode
- NFC feature can be switched off/on by the user
- NFC needs close proximity – proximity by user consent
- Idle timeout planned

- ... And further features as for contact EstEID
## EstEID Token Overview

<table>
<thead>
<tr>
<th>Token Model</th>
<th>Electronic function</th>
<th>Physical function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identification I</td>
<td>Authentication A</td>
</tr>
<tr>
<td></td>
<td>Signing S</td>
<td>Encryption E</td>
</tr>
<tr>
<td></td>
<td>Identification PI</td>
<td>Travel Doc TD</td>
</tr>
<tr>
<td>eID</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>eRP</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Digi-ID</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NFC Digi-ID</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mobile-ID</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

- **X** indicates the token has the function.
- **(X)** indicates the token has the function, but only in a limited way.

© 2008 Trüb Baltic AS – www.trueb.ee
EstEID Chip Application – Development Outlook #1

• Trusted elements in using EstEID
• Untrusted environment

=> Trusted Environment Verification
=> User Presence Verification
EstEID Chip Application – Development Outlook #2

• Near Future:
  Human Being Verification

• Distant Future 2
  Owner Verification

• Undetermined Future
  Using free memory space for offline use
  i.e. facial picture for loyalty purposes
Questions & Answers

Or

Comments & Suggestions

Now or later to

andreas.lehmann@trueb.ee

Thank you!