Cybernetica AS

- Cybernetica is a R&D intensive ICT company
  - Established 1997 based on Institute of Cybernetics
  - Personnel: 170 employees, 10% with PhD
  - Offices located in Tallinn and Tartu
  - Integrated Management System: ISO 9001 and ISO 27001
  - Research cooperation with DARPA and EU

- Behind much of e-Estonia: digital signature law, ID card, X-Road, e-Police, e-Customs, Internet voting, SmartID, ...

- Has received various international and national acknowledgements
What is X-Road?

- Technology for governmental e-services backbone
  - Scalable and secure
  - Supports collaboration and cooperation
- Dual usage
  - Delivery platform for citizens e-services
  - Platform for governmental data exchange and business processes automation
Why is X-Road Interesting?

- A complete, working system
  - PKI
  - Digital signatures
  - Long-term validity
  - Covers all the bases

- An example of trade-offs between security goals
  - e.g., performance vs. long term validity

- Mix of technical and organizational security measures
Brief History

- 2001 – first version of X-Road goes live
- 2002 – v2, SOAP support, asynchronous messages
- 2003 – v3, SOAP attachments, access control groups
- 2005 – v4, message log encryption, secure e-mail (removed in v5)
- 2010 – v5, web UI, Document/Literal encoding, Ubuntu support
- 2012 – beginning of UXP product development: new generation targeting international users
- 2015 – v6, based on UXP technology. Rewrite of the system
- 2018 – X-Road development transferred to NIIS
- Currently two forks: UXP by Cybernetica, X-Road by NIIS
X-Road Overview

● X-Road provides secure, unified transport protocol for web services

● Distributed architecture
  – Organizations have control over their data
  – No central database (no “big brother”)

● Supports heterogeneous systems
  – Works well with legacy systems
  – Does not need (major) changes to legislation and organizational structure
X-Road Overview (2)

- **Secure**
  - Uses strong authentication
  - All traffic over encrypted channel
  - Digital signing, time stamping and audit logging create accountability

- **Scalable, resilient**
  - No central bottlenecks
  - No single points of failure
  - All the components can be made redundant
A Digital Ecosystem
System Architecture
System Architecture
System Architecture
Important Features

- Communication is peer to peer
  - End to end encryption between organizations
  - Nobody but the communicating organizations can see the data
- Data owner sets the rules
  - Sets requirements for data users
  - Manages access control rights
- Communication is implemented as web services
  - SOAP protocol is used between security servers and organization information system
  - Adapters can be used to interface with existing information systems
The Importance of Services

- All the data access is via services
- Service encapsulate the storage and implementation details
- Services provide limited view on data
  - Limit on search fields
  - Limit on output fields
  - Business rules can be applied on input or output
- Different services can be developed for different clients
- The data owner is responsible for developing services
Authentication and Access Control

- All data access must be authenticated and access control rules must be applied

- Create central database of persons' access rights?
  - Who are the data sources?
  - Who updates the data?

- Do we offer end-to-end security?
  - What about legacy systems?
More on Authentication

- The user invokes the service though her employer's IS
  - Technically, the IS can always impersonate the user
- The service provider does not know anything about the end user
  - Users and their roles are defined in the client organization
Two-Level Access Control

- The X-Road core deals only with inter-organizational access control, where access is granted to an organization as a whole
- The client organization must ensure that only right people can use the service, by using whatever technical means it sees appropriate
- This obligation is enforced by service provisioning contract between the organizations
- Before joining X-Road, a client organization must prove that it has implemented suitable authentication and access control mechanism
  - Ideally, the information system should be audited by external auditor
Two-Level Access Control (2)

- Two-level access control isolates the details of organizational authentication and access control mechanisms
- The impact to the existing systems is minimized
- Balanced use of technical and organizational security measures
Additional Controls

- Monitoring – query statistics are sent to monitoring system
  - Can be viewed by security server administrator and central administrator
  - Can be used to discover usage that does not correspond to normal usage patterns

- Public query log – registries keep log of queries
  - Can be viewed by citizens via citizen portal
<table>
<thead>
<tr>
<th>Kuupäev</th>
<th>Kirjeldus</th>
<th>Päringu sooritanud asutus</th>
<th>Toimiku nr</th>
<th>Päringu sooritanud isik</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.08.2004</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>01.09.2004</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>31.07.2007</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>07.02.2008</td>
<td>Isikuandmed ja pildid KMA IS-IS</td>
<td>Notarite Koda</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>11.02.2008</td>
<td>Isikuandmed ja pildid KMA IS-IS</td>
<td>Notarite Koda</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>02.05.2009</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>02.05.2009</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>02.07.2011</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>02.10.2012</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
<tr>
<td>19.01.2013</td>
<td></td>
<td>Koodikutportaal</td>
<td>1</td>
<td>37607310312</td>
</tr>
</tbody>
</table>
In Case of Incident

- X-Road signatures can be used to prove actions between organizations
  - For example, service provider can prove that the query originated from the client organization

- When necessary, organizations must implement measures to prove actions of users
  - Audit logs
  - End-user digital signatures
Takeaways

- Cryptography solves many problems, but not all
  - Always know what some technology really provides and what are the assumptions
- You always need some organizational security measures
- Imperfect system that works/is used is better than perfect system that doesn’t
Thank you!

Cybernetica AS
Mäealuse 2/1, 12618 Tallinn, Estonia
info@cyber.ee    www.cyber.ee