The State ICT Infrastructure in Estonia

Hannes Kiivet, Domain Manager, Estonian Information System Authority
Agenda

• e-State unique aspects, risks and challenges
• Estonian State ICT infrastructure
• X-road’s importance for a well-functioning e-State
Welcome to e-Estonia. Let’s zoom in...
Let’s zoom in a little more...
Everything starts with people
My background

• Education: management of IT, MBA
• 9+ years in RIA
• Positions held:
  ■ service manager
  ■ domain manager
  ■ head of development
  ■ head of interoperability solutions
  ■ advisor
  ■ domain manager (current)
State data governance domain

Vision:
• We enable government data reuse

Services:
• catalogue of information systems and data
• data and document exchange platform
• data governance requirements evaluation
Information System Authority (RIA)

- Develop and manage central e-government components
- Coordinate national cyber security
- Distribute EU structural funds for IT development
Organisation chart of e-government

- Government of Estonia (IT-advisor)
  - Ministry of Economic Affairs and Communications (CIO + government CIO + 3 departments)
    - Information System Authority
  - Ministry X (CIO)
    - IT development center
  - Ministry Y (IT department)
  - Local governments (IT department/guy)
    - ...

Estonian way of life

- 500 million digital signatures given
- 700 million electronic log ins
- 95% of taxes are declared online
- 98% medical prescriptions digital
- 1/3 of votes cast online
- Estimated 2-6% of GDP saved
How to get to the e-State?
<table>
<thead>
<tr>
<th>e-State</th>
<th>vs</th>
<th>conventional state</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Who is behind the computer?</td>
<td>• Who is behind the counter?</td>
<td>• Who is behind the counter?</td>
</tr>
<tr>
<td>• Who signed the document?</td>
<td>• No problem: the citizen is in your office</td>
<td>• No problem: the citizen is in your office</td>
</tr>
<tr>
<td>• How to securely exchange electronic data?</td>
<td>• How to transport/manage paperfolders in-house and between institutions?</td>
<td>• How to transport/manage paperfolders in-house and between institutions?</td>
</tr>
<tr>
<td>• Who owns data X?</td>
<td>• No worries: ask the citizen</td>
<td>• No worries: ask the citizen</td>
</tr>
<tr>
<td>• How to best serve citizens in whole-of-governement view?</td>
<td>• How to serve my customer?</td>
<td>• How to serve my customer?</td>
</tr>
</tbody>
</table>
Risks and challenges

• No fallback (going back to analogue)
• Possibility to develop too complex systems:
  ■ maintainance costs rising
  ■ dependence of central components
  ■ vendor lock-in
  ■ low freedom in technology decisions
• Cyber incidents:
  ■ interuptions to real life/services
  ■ loss of trust of IT systems and/or users
Estonian digital enablers

- Trust & cooperation between stakeholders
- Systematic capacity building: Tiger Leap & Look@World projects
- Relatively high level of awareness
- Critical competences
The Foundation

- Authentication of people in digital environment + digital signature
  - electronic identity
  - digital signature

- Secure/standardized identification and data exchange of information systems
  - data exchange platform X-Road
Plastic + electronic identity (ID-card)

• Compulsory for all residents
• One person = one identity

Use cases:
• Authentication
• Legally binding signature
• File encryption/decryption for secure delivery
Data exchange platform (X-Road)

- Distributed environment of interoperability for information systems with central identity management
- 15 years of continuous operations
- Overview of the entire ecosystem, incl activity between parties
- Interoperable, resource efficient and flexible
Once only principle (OOP)

- Citizen must enter information only once
- Information collected to the state information system must be reusable and reused
Catalogue of systems (RIHA)

- Complete picture of members and services
- Avoids double solutions and data collection
- Control over compliance with the law
Reference security framework (ISKE)

- A set of organisational, infrastructural/physical and technical security measures
- Based on German *IT-Grundschatz*
- 3 aspects of security: availability, confidentiality and integrity of data
- 3 levels of security requirements
- Auditing every 2...4 years
This looks nice! How does it work exactly?
Estonia IT-architecture example (functional view)

Who is this person?

e-Police information system

Police officer
Estonia IT-architecture example (functional view)

Population registry

Catalogue of systems

Where is data about persons?

e-Police information system

Who is this person?

Police officer
Population registry

Catalogue of systems

What are the inputs and outputs?

Request

Response

e-Police information system

Police officer

Who is this person?
Estonia IT-architecture example (functional view)

Catalogue of systems

Population registry

Secure channel

Response

e-Police information system

Police officer

Who is this person?
Estonia IT-architecture example (functional view)

Who used my data?

Citizen

Population registry

Catalogue of systems

Request

Response

Secure channel

e-Police information system

Police officer
Estonia IT-architecture example (functional view)

Who used my data?

Citizen → Population registry → Secure channel → e-Police information system → Police officer

Catalogue of systems

Request → Response
Estonia IT-architecture example (governance view)

- Catalogue of systems
- Population registry
- Secure channel
- RIA
- Response
- e-Police information system
- Police and Border Guard Board

Ministry of Internal Affairs
Everything’s perfect in Estonia?
Estonian ID-card case

Problem:
• Global flaw in RSA crypto library, affecting 1 billion smartchips (including Austrian, Slovakian and Spanish cards)
• Theoretical vulnerability in 750,000 Estonian ID-cards (60% of those in circulation)

Solution:
• Open communication
• Private keys suspended in November, revoked in April
• Bypass the problem with remote updating/generation of new keys during 6 months
• Result: 95% electronically used cards renewed online
Souvenirs?
# Lessons to be learned

<table>
<thead>
<tr>
<th>Do:</th>
<th>Don’t:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Copy best ideas and solutions</td>
<td>1. Don’t reinvent the wheel</td>
</tr>
<tr>
<td>2. Maintain parties’ technology freedom/autonomy</td>
<td>2. Don’t build central systems</td>
</tr>
<tr>
<td>3. Access others’ data from only baseregistries</td>
<td>3. Don’t keep your baseregistries closed</td>
</tr>
<tr>
<td>4. Create resilient electronic identities and enable digital</td>
<td>4. Don’t rely on insecure authentication of users, institutions and</td>
</tr>
<tr>
<td>signatures</td>
<td>companies</td>
</tr>
</tbody>
</table>
Earn the trust of citizens and execution is a magnitude easier.
Thank You for listening!
Any questions?

Hannes Kiivet
hannes.kiivet@ria.ee