IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGIES IN ESTONIAN GOVERNMENT

Jaan Priisalu

Topics

1. Challenge of Estonia
2. History of cyber cooperation
3. What we defend?
4. Government infrastructure
5. Blockchain functions
6. Use cases of blockchain


ESTONIA

Historical milestones

1960 - Institute of Cybernetics

1991 – Independence from Soviet Union

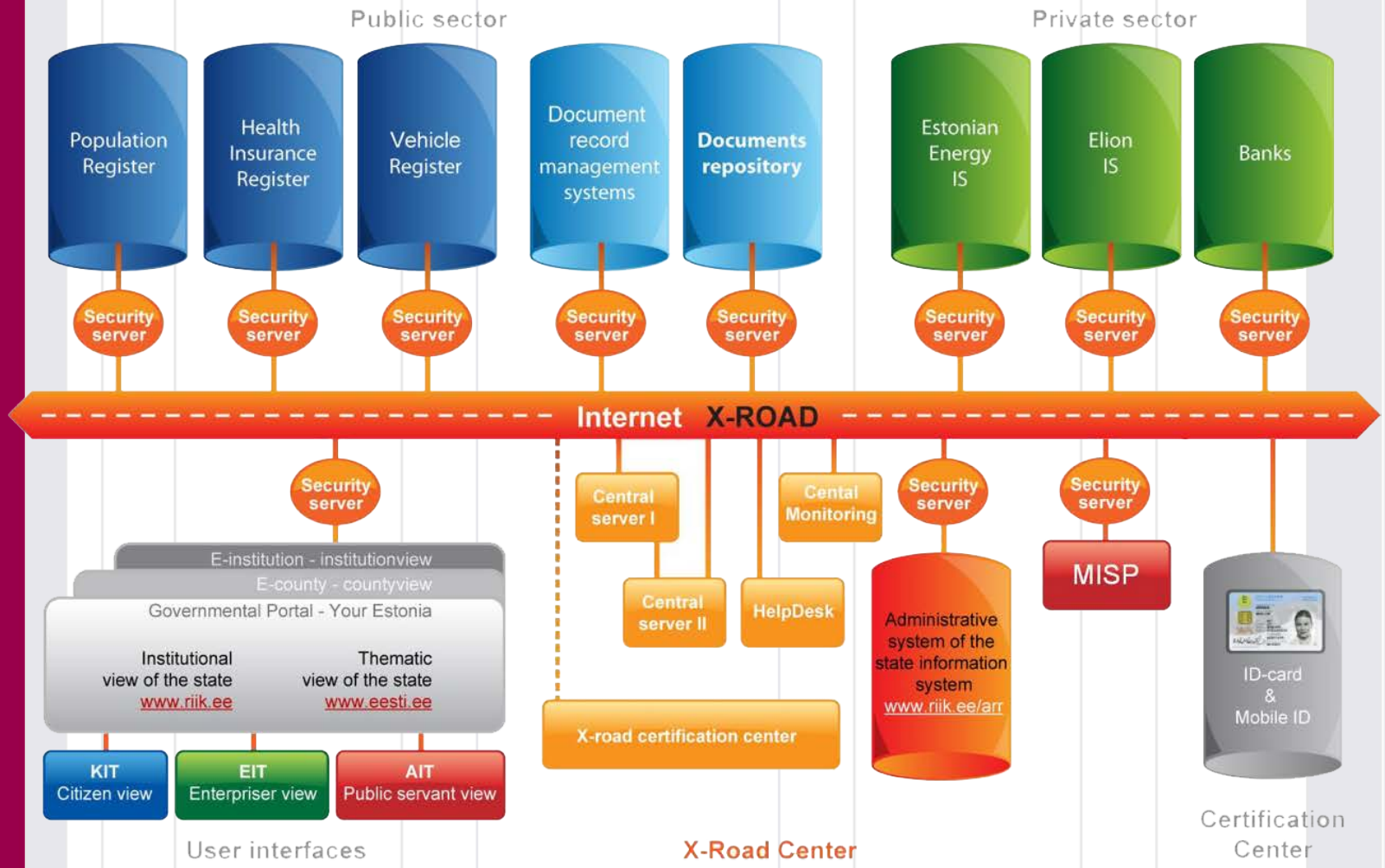
1998 – Cooperation of banks
2000 - Digital Signature Law
2003 – Cybercrime Industry
2005 - E-voting
2006 - CERT-EE
2007 - “Bronze riots“
2008 - NATO CCDCOE
2008 - National Cyber-Security Strategy
2009 - Cyber Defence subunits
2011 - Cyber Defence Unit
2012 – Cabinet level exercise
2014 – New Strategy

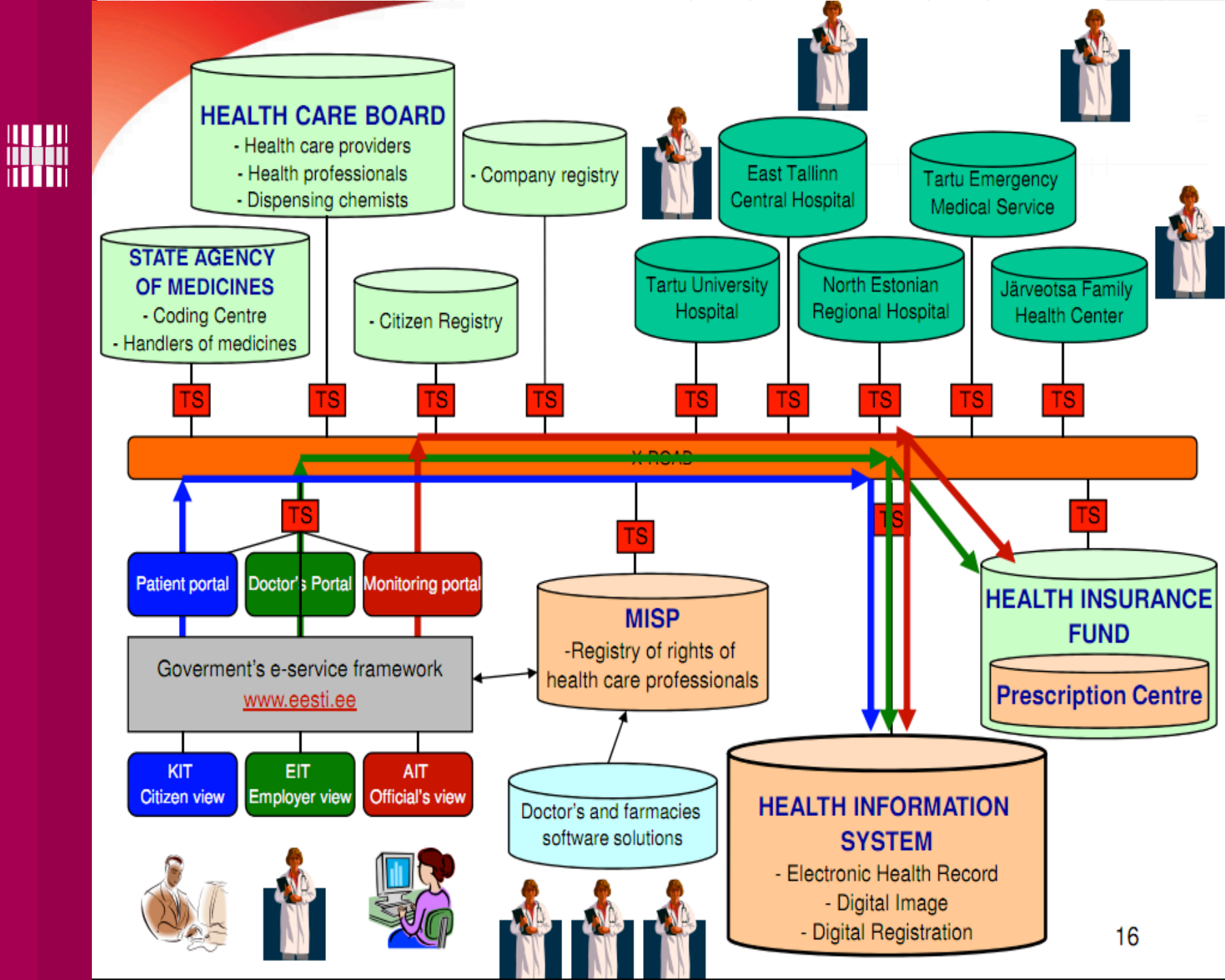
Way of life

Defending an e-way of life

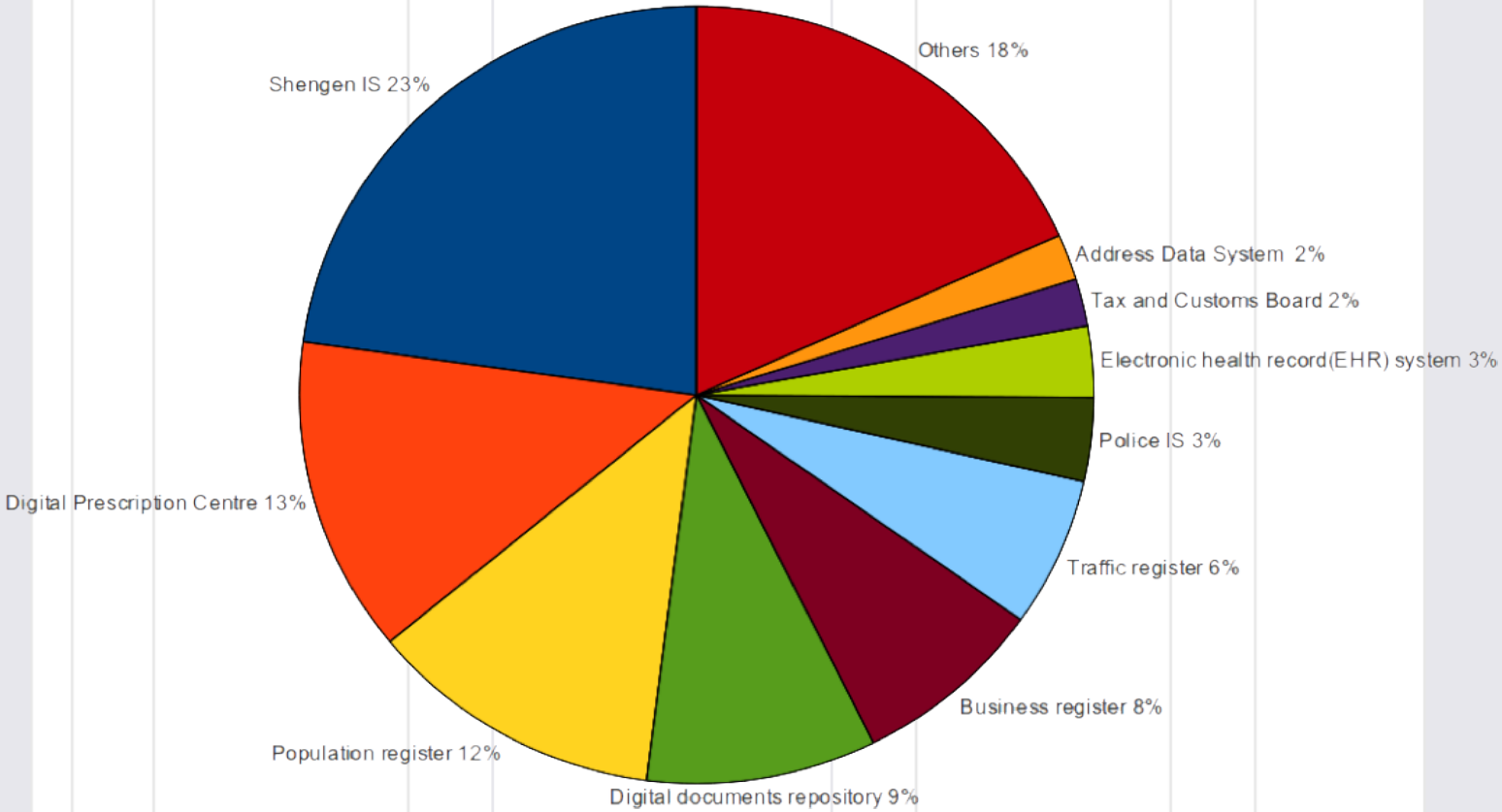
- E-stonia – ecosystem
- E-solutions widely in use and dependable
  - 99% of banking transactions are electronic
  - 96% tax declarations are electronic
  - M-parking
  - National ID cards issued
  - Sign and encrypt documents using E-ID
  - E- & M-voting
  - National Electronic Health Records
  - Public transport ID-ticket, ID-fishing licenses etc etc

Estonian information system

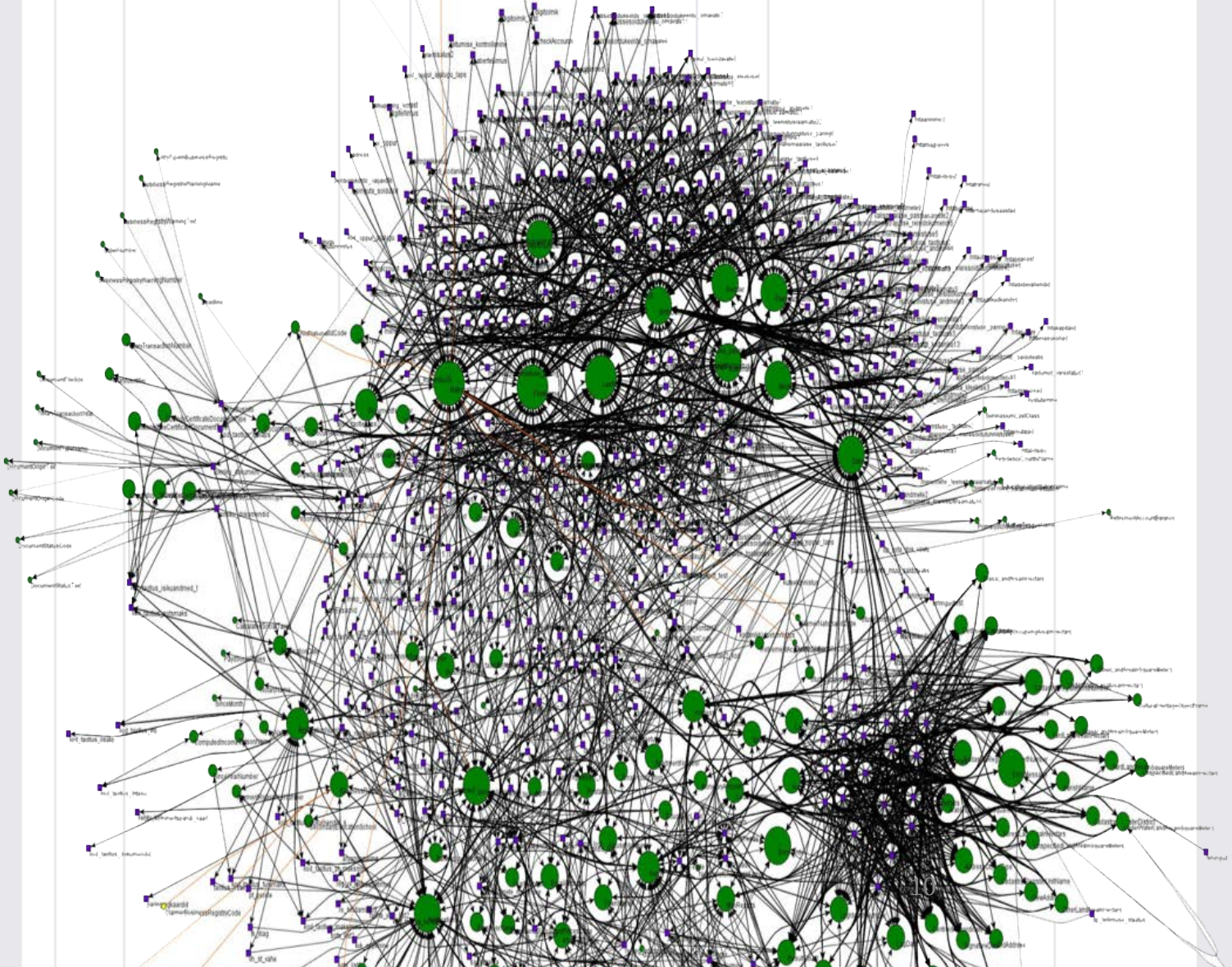



HEALTH CARE BOARD
- Health care providers
- Health professionals
- Dispensing chemists
- Company registry
East Tallinn Central Hospital
Tartu Emergency Medical Service
STATE AGENCY OF MEDICINES
- Coding Centre
- Handlers of medicines
- Citizen Registry
Tartu University Hospital
North Estonian Regional Hospital
Järveotsa Family Health Center
TS
X-ROAD
Patient portal
Doctor's Portal
Monitoring portal
Goverment's e-service framework
www.eesti.ee
KIT
Citizen view
EIT
Employer view
AIT
Official's view
MISP
-Registry of rights of health care professionals
HEALTH INSURANCE FUND
Prescription Centre
Doctor's and farmacies software solutions
HEALTH INFORMATION SYSTEM
- Electronic Health Record
- Digital Image
- Digital Registration

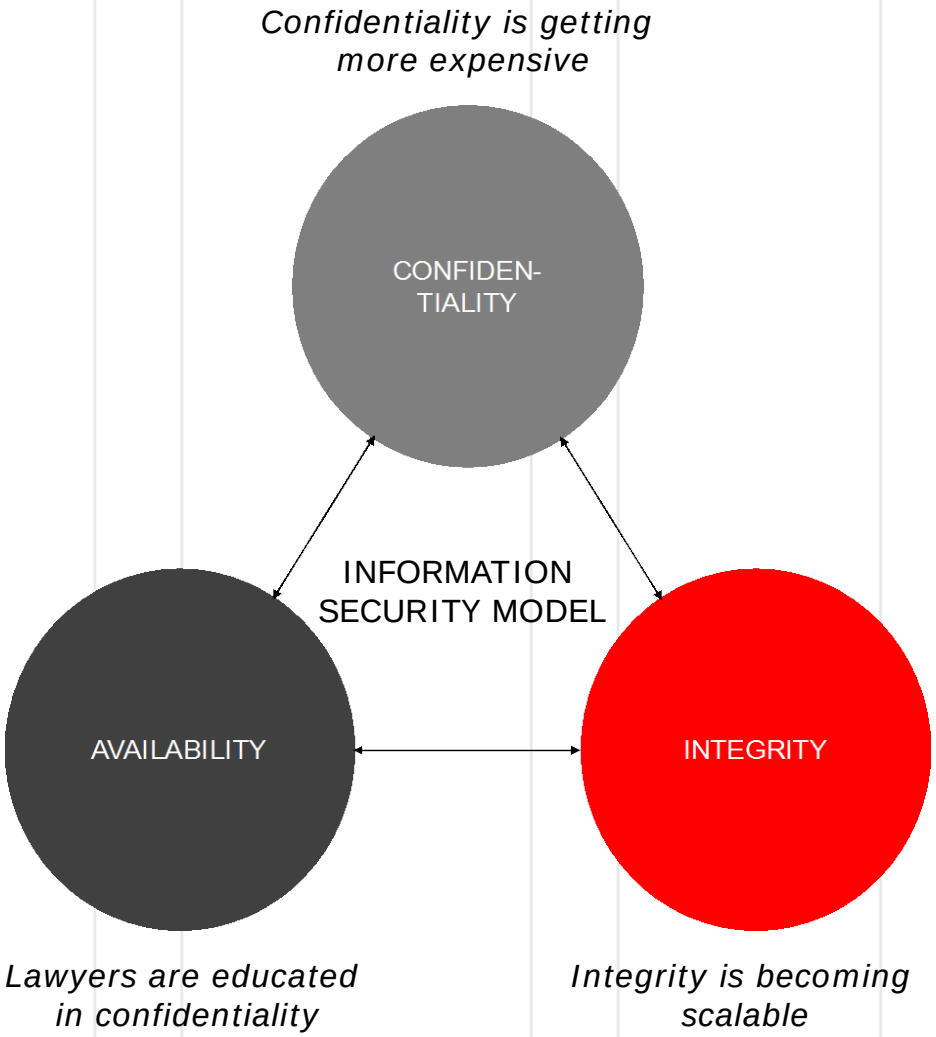
Service transactions in X-Road by providers



X-Road has no center



CIA Triad


Confidentiality is getting more expensive
CONFIDEN-TIALITY
INFORMATION SECURITY MODEL
AVAILABILITY
INTEGRITY
Lawyers are educated in confidentiality
Integrity is becoming scalable

Blockchain

- When considering blockchain we touch components:
  - Time integrity proof
  - Widely witnessed consensus
  - Distributed immutable database
  - Predicate calculation machine
  - Distributed ledger
  - Digital money
- NB! Distributed is not equal to public
- Most interesting for government is immutable database

Digital history

- Estonia has 15 years of digital history
- Most of documents have no paper original
- Government activity has to be archived, proof value preserved
- Signature algorithms are amortizing but proof value have to be preserved
- Wrapping document into blockchain preserves proof value

Registry integrity

- Registry is primary source of rights in Estonia
  - documents are secondary
- Integrity of registry entries is vital
- Blockchain provides immutability
- Implementation started with
  - Official Announcements
  - Marital property registry

Activity records

- Investigation needs reliable activity traces
- Source of activity is not always disputed – PKI mostly redundant
- Implemented on:
  - System logs (syslog servers)
  - X-road transaction logs (upgrade from hashchains)

Fighting intruders

- It’s again all about Integrity!
  - APT – persistent means network device integrity loss
  - Erasing traces is integrity loss
  - Software update has to guarantee code integrity
- IoT is aggravating the problem
- Experimenting with malware means you have to guarantee isolation!

Virtual country

- There are 3 things not possible in digital channels
- We can continue the state even under occupation
  1. Cold backup somewhere else
  2. Warm backup to continue operations
  3. Digital Embassy to provide network security by Vienna convention
  4. Distributed state in clouds
     - Digital signatures
     - Personal encryption keys
     - Multiparty computation
     - Blockchain to prevent manipulation
- E-citizenship creates backup capacity in foreign states

Combining technologies

- Blockchain complements PKI
- Signatures need time proofs
- Quantum immune non-PKI signatures could be built on time proofs
- PKI based timestamp and blockchain can be used in parallel

Summary

- Big distributed digital system must prevent malicious modifications. It means - provide integrity!
- The best technology to provide scalable integrity today is blockchain.

Thank you!