REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

European Union
European Regional
Development Fund

Investing
in your future

Document Exchange Protocol DHX

Priit Parmakson

May 2, 2016

Document exchange protocol DHX

Developed by Estonian Information System Authority in 2015-2016

Purpose
standardised and simple method to exchange documents

Target group
all Estonian public sector organisations (mandatory)
companies who have a lot of business with public sector (optional)

Motivation

Document Exchange Centre (DEC)
https://www.ria.ee/en/dec.html

- operated 10+ years
- over 600 agencies
- uses X-Road as transport layer
- centralised, “main post office“ type solution

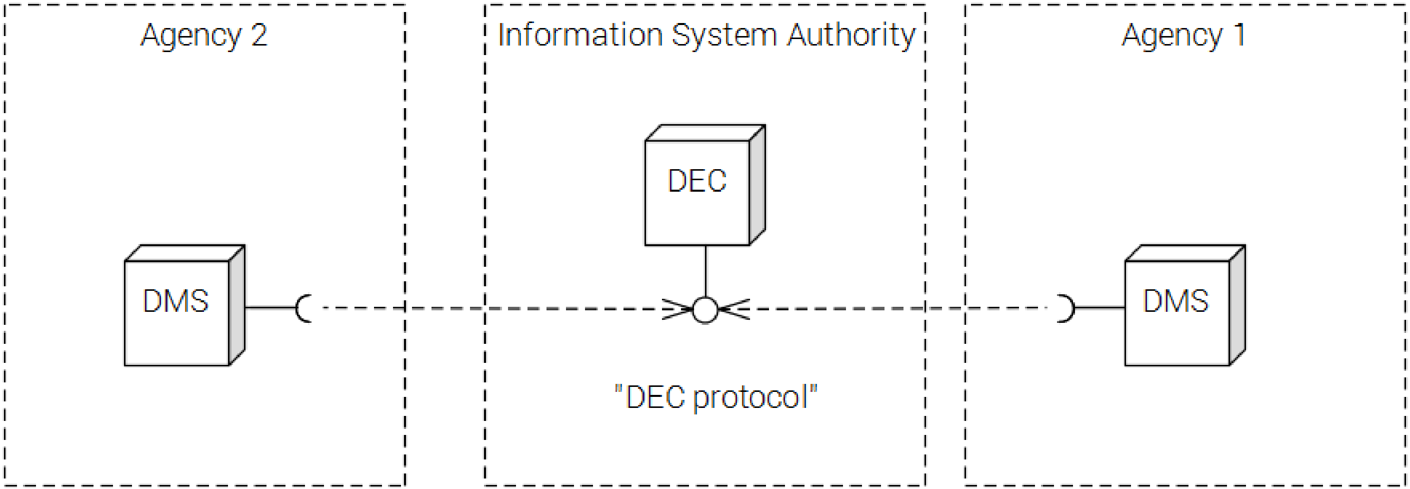
Need:

- faster and simpler document ecxhange
- lower operating costs
- no single point of failure

Architecture

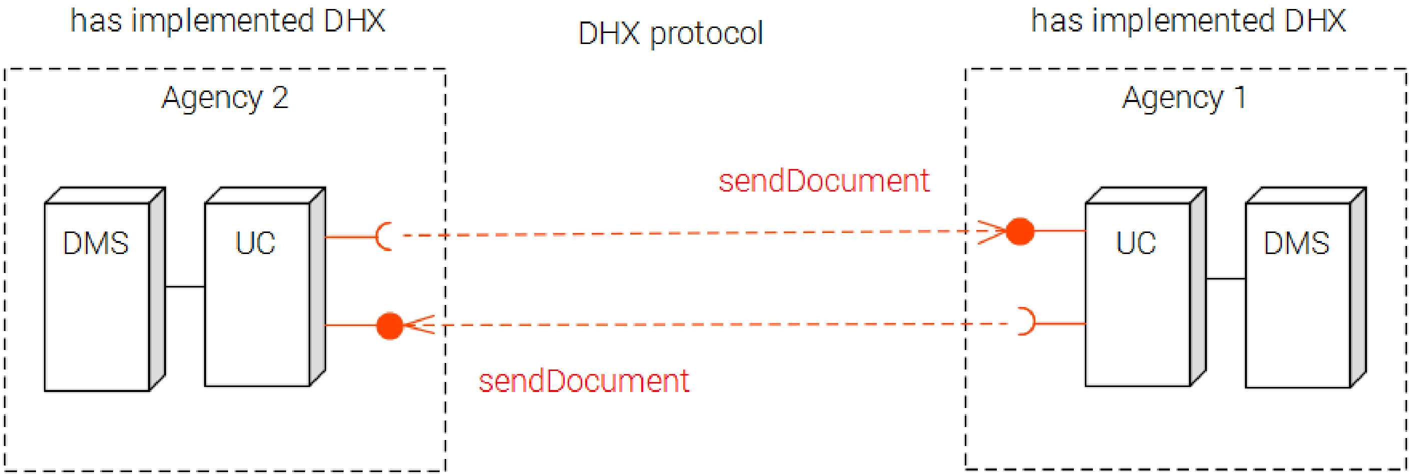
- symmetric interaction with no central node
- a thin layer on top of X-Road
- a thin layer under Document Metadata Standard („the Capsule“)
- made to fully use the new capabilities of X-Road v6
- reliable delivery
- strong e-identity
- encryption
- low implementation costs
- low operation costs
- structured as protocol + reference implementation + standardised adapter
- developed by following the best practice of protocol design and specification

As is



DMS - Document Management System; DEC - Document Exchange Centre

To be



UC - Universal Component

X-ROAD

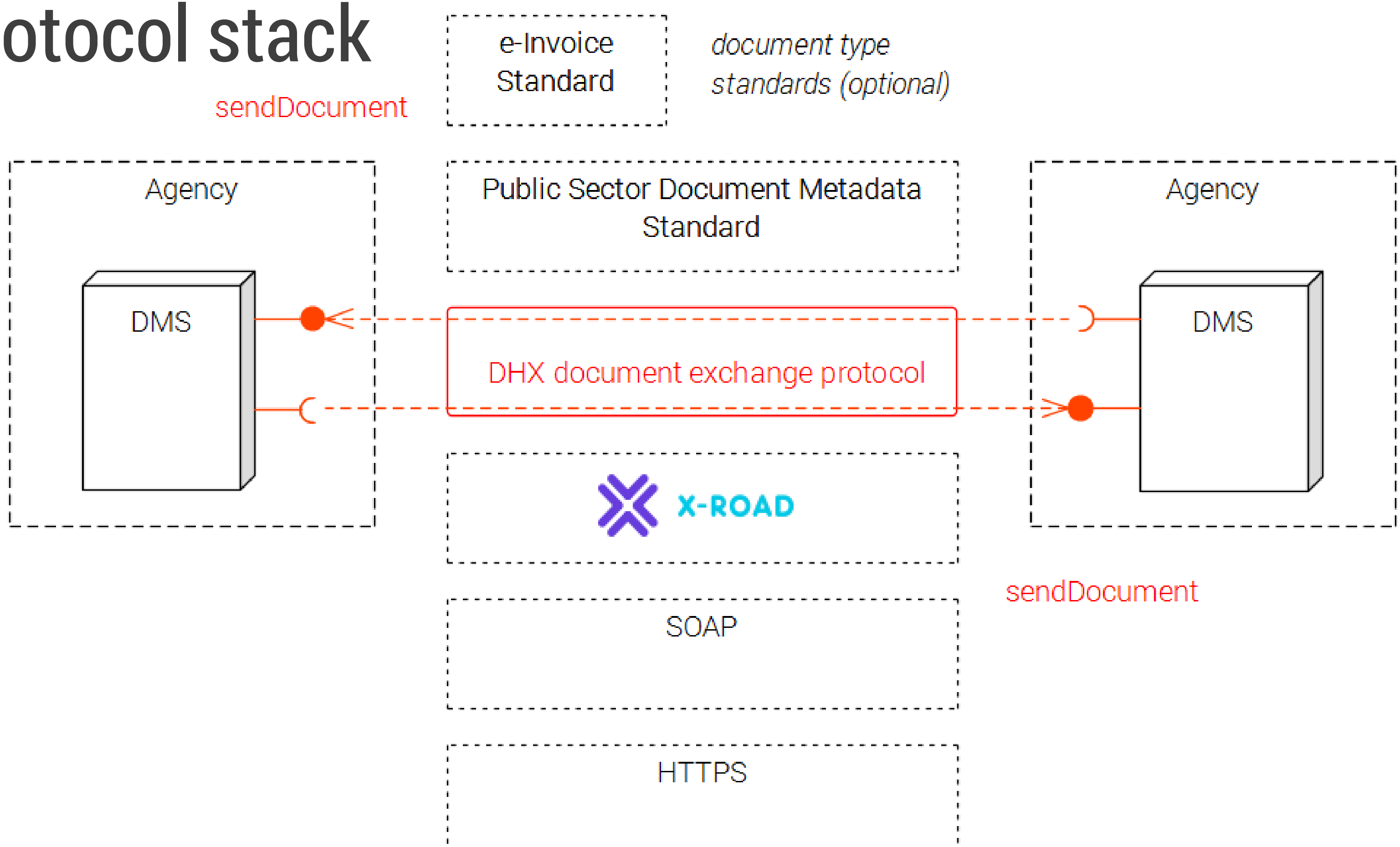
Builds on unique capabilities of X-Road

X-Road, the Estonian national public sector data exchange layer

- addressability
- service discovery
- strong identity
- security
- legally binding
- non-repudiation

X-ROAD

Protocol stack



sendDocument

e-Invoice Standard

document type standards (optional)

Agency

Public Sector Document Metadata Standard

Agency

DMS

DHX document exchange protocol

DMS

X-ROAD

sendDocument

SOAP

HTTPS

Elements of DHX

- DHX standardised web service
- name rule
- message format: Estonian Document Metadata Standard ("the Capsule")
- processing rules
- provisions for the transition period

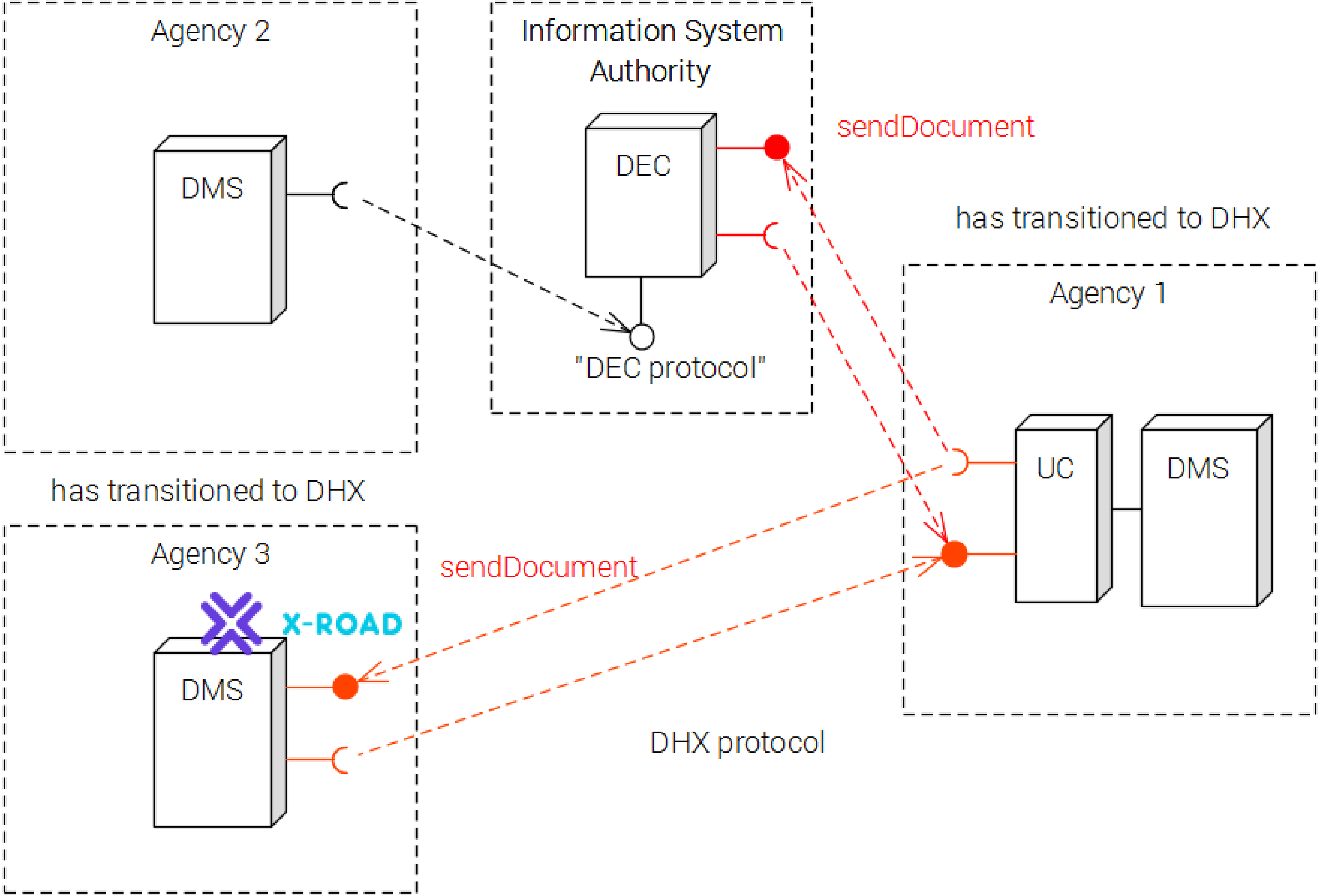
Implementer support

- reference implementation
- standardised adapter component (optional)

Schedule

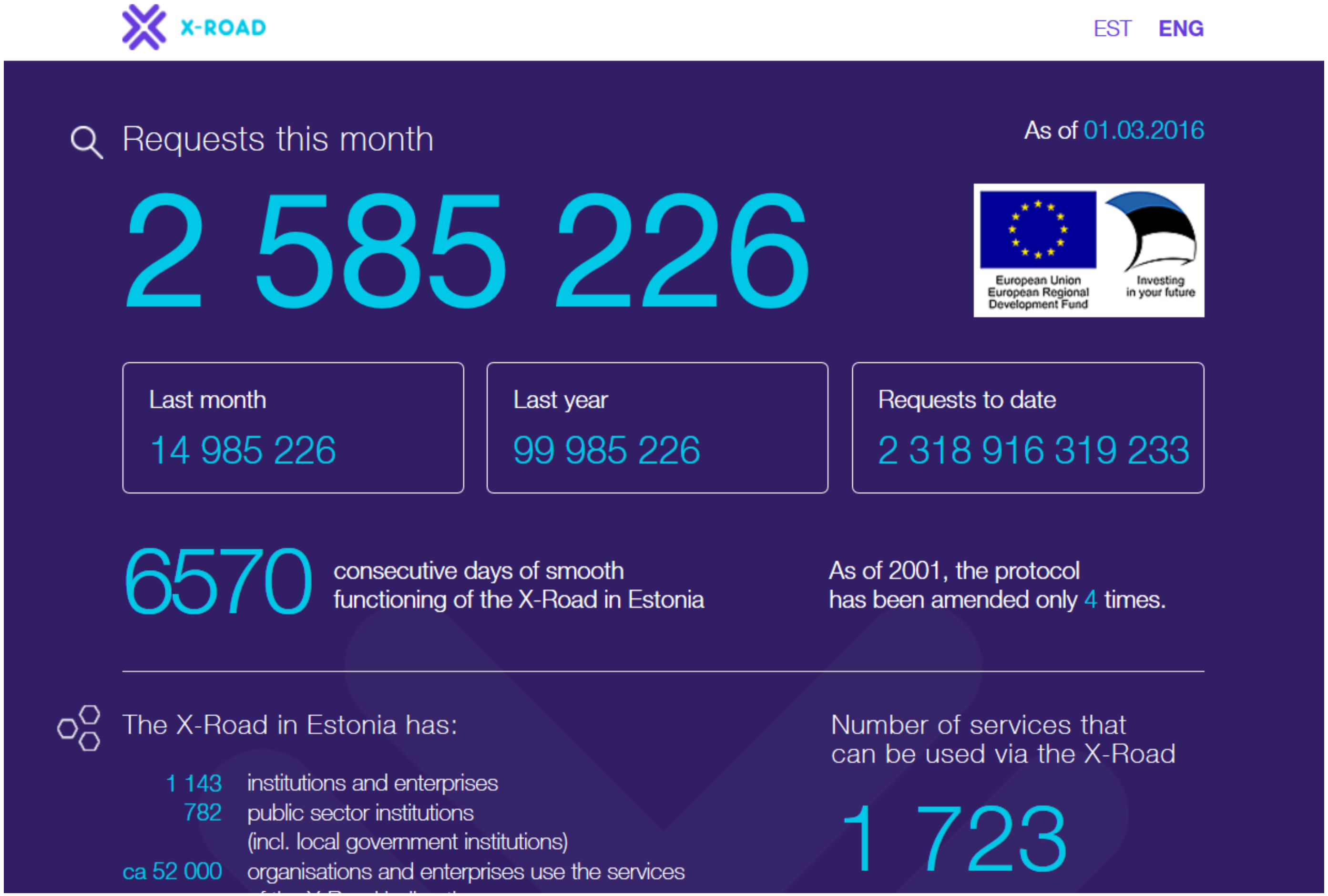
2015	Draft version of the protocol
	https://github.com/e-gov/DHX
2016	Reference implementation
	Verification
	Development of universal adapter component
	Migration planning
2017-2018	Migration to DHX

Transition


Agency 2
DMS
Information System Authority
DEC
sendDocument
"DEC protocol"
has transitioned to DHX
Agency 1
UC
DMS
has transitioned to DHX
Agency 3
sendDocument
X-ROAD
DMS
DHX protocol

Brief overview of X-Road

X-ROAD



Requests this month

As of 01.03.2016

2 585 226

Last month	Last year	Requests to date
14 985 226	99 985 226	2 318 916 319 233

6570 consecutive days of smooth functioning of the X-Road in Estonia

As of 2001, the protocol has been amended only 4 times.

The X-Road in Estonia has:

1 143	institutions and enterprises
782	public sector institutions (incl. local government institutions)
ca 52 000	organisations and enterprises use the services

Number of services that can be used via the X-Road

1 723

The X-Road in Estonia has:

1 143	institutions and enterprises
782	public sector institutions (incl. local government institutions)
ca 52 000	organisations and enterprises use the services of the X-Road indirectly
1 169	interfaced information systems
220	security servers installed by members

Number of services that can be used via the X-Road

1 723

Every party who provides services offers 8 services on average

Designed to be secure

Traditional attacking vectors cannot be used with the X-Road due to its structure and architecture

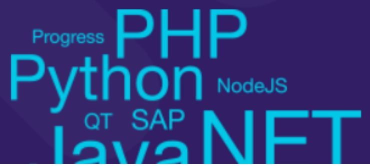
X-Road implements the following security technologies

XAdES, ASiC, VPN, RSA, TSL, RFC3161, OCSP, PKI

5 most popular service providers

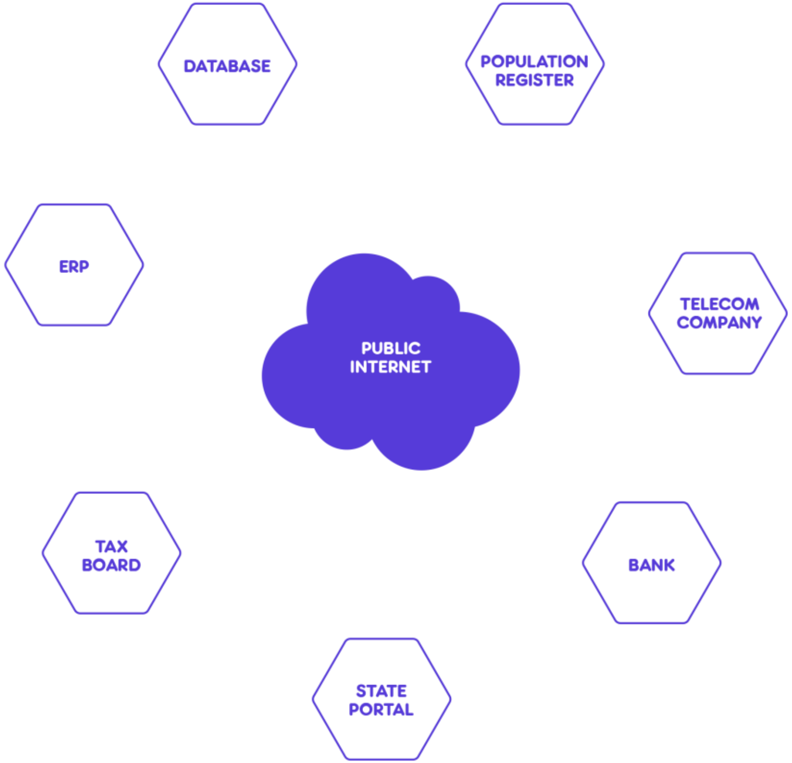
139 253 983	Estonian Tax and Customs Board
65 935 244	Population Register
50 298 345	Prescription Centre
38 240 423	Official Announcements
33 071 481	e-File

Most popular platforms of information systems that have been interfaced with the X-Road



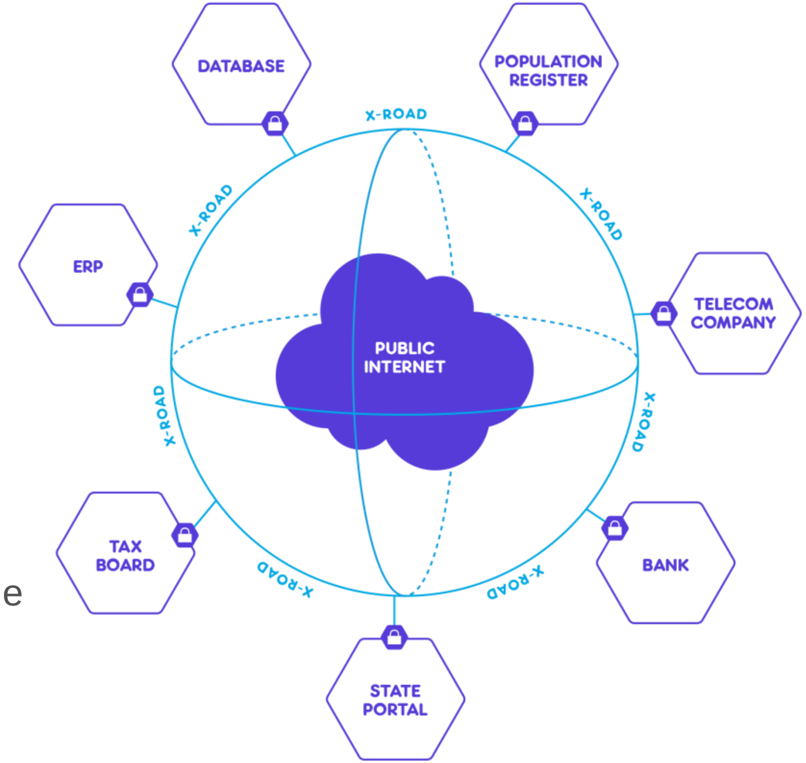
Starting point

- Everyone is aware of their internal processes
- Everyone is in the network
- Security of data exchange



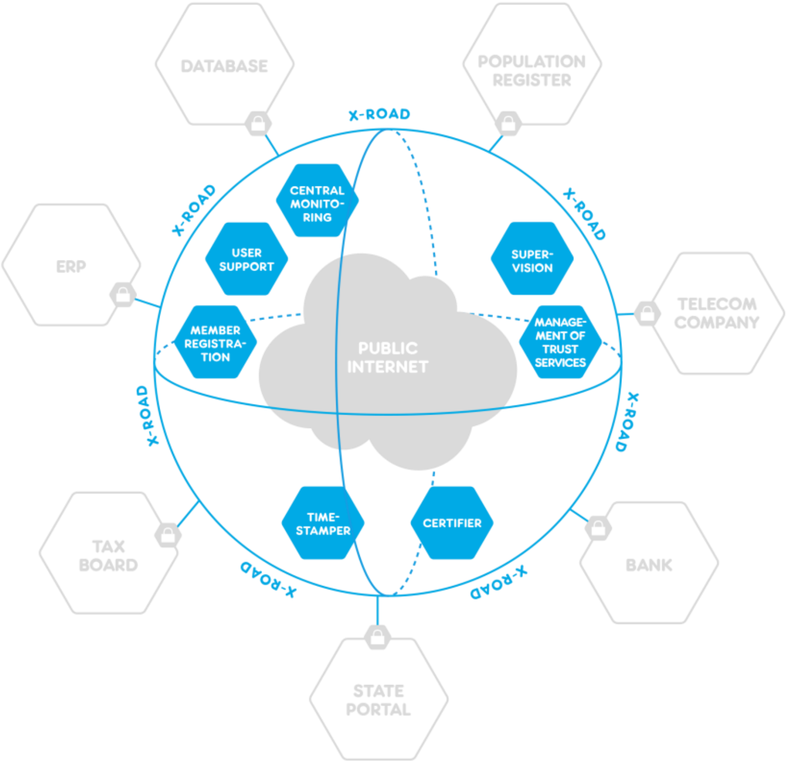
X-Road: organisation method
# of a distributed state information system

- Uses the internet
- Maintains freedom for its members
- Ensures the authenticity of members
- Provides means for secure information exchange



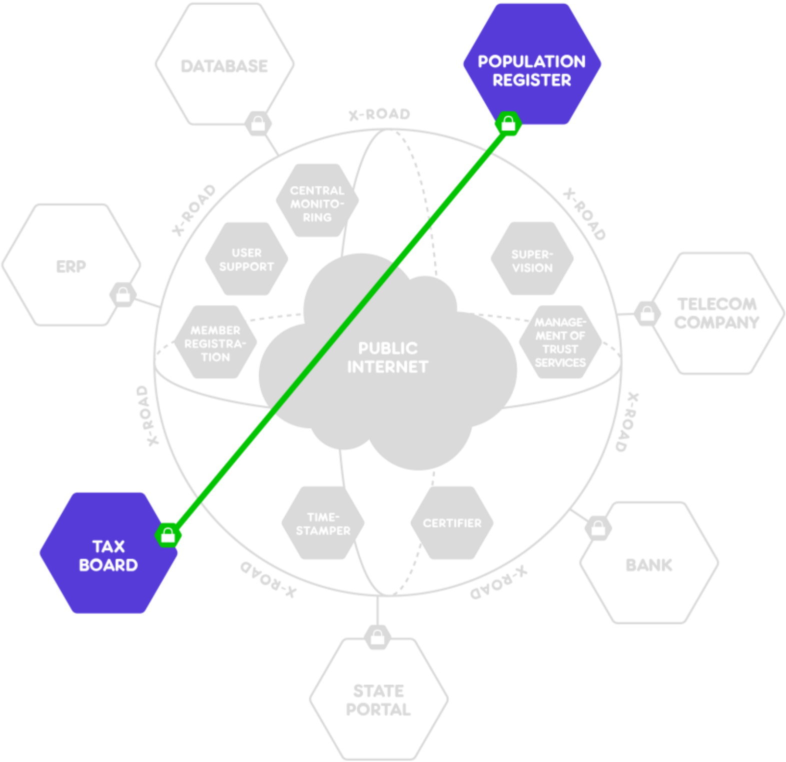
X-Road Centre

- Registration of members
- User support
- Central monitoring
- Supervision
- Management of trust services
- Timestamp and certification service



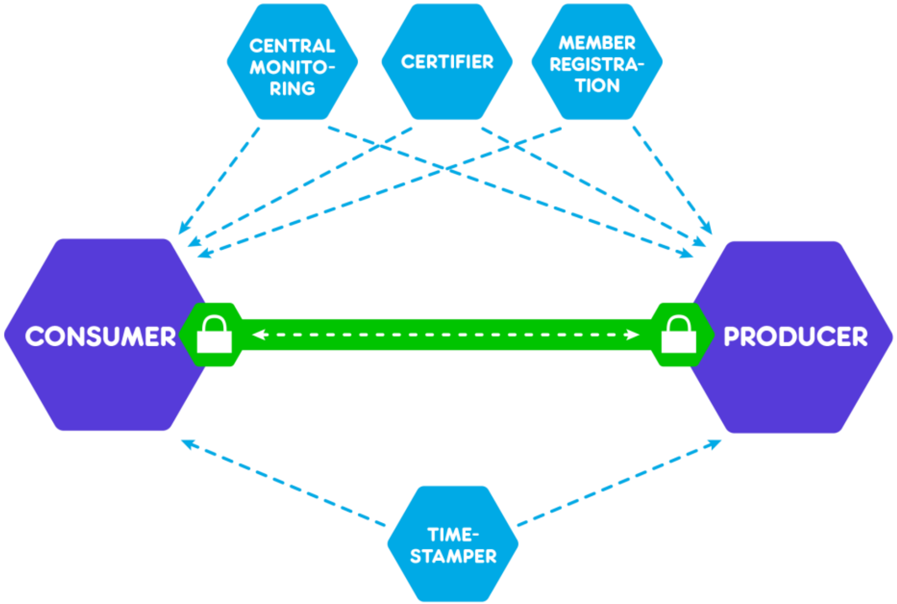
Data does not pass through X-Road Centre

- Universal membership
- Freedom of choice
- Direct communication



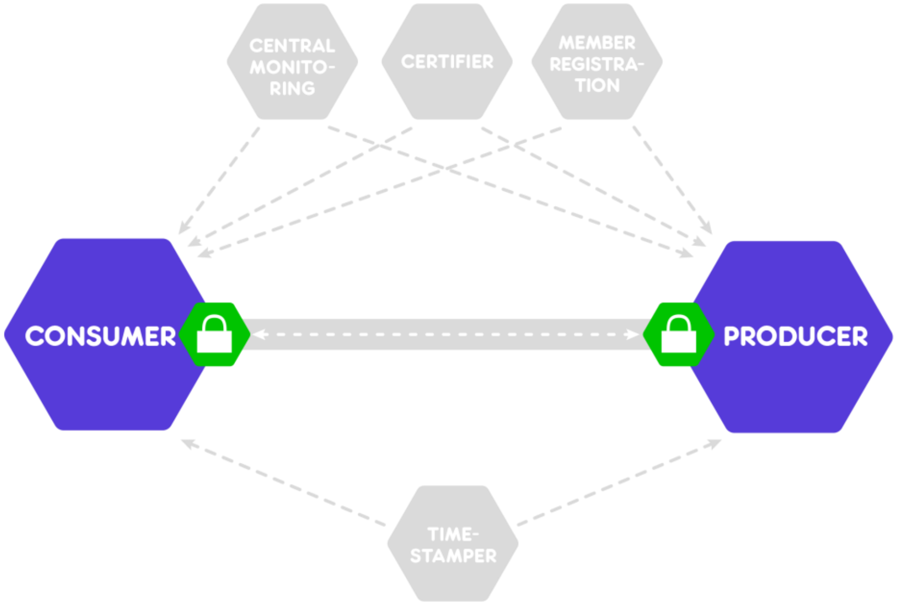
Overview of communication/ data exhange

- Availability
- Integrity
- Confidentiality



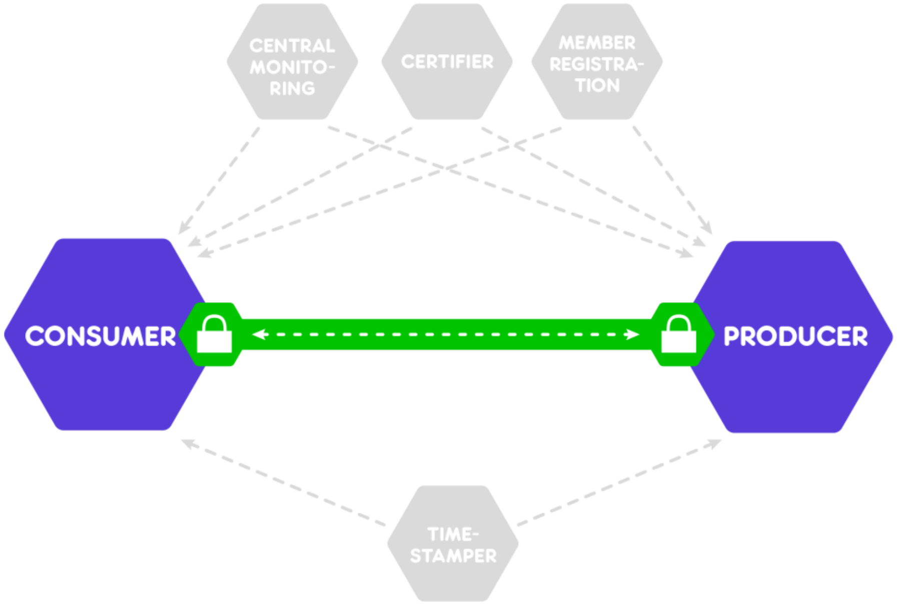
Services and access rights

- Describing the service
- Providing access rights



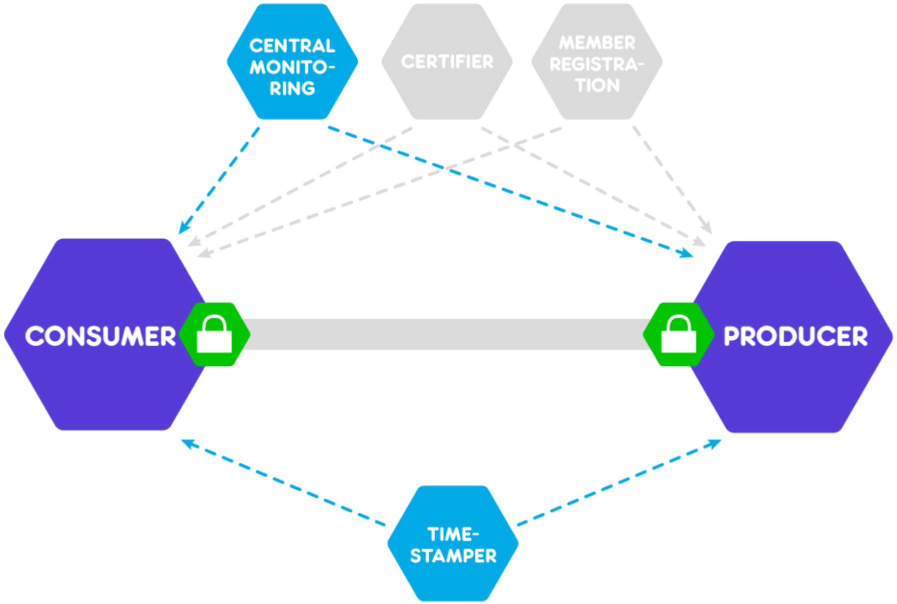
During a transaction

- Signing/stamping a request
- Creating an encrypted channel
- Verifying a signature/stamp
- Signing/stamping a response
- Sending a response
- Verifying a response signature



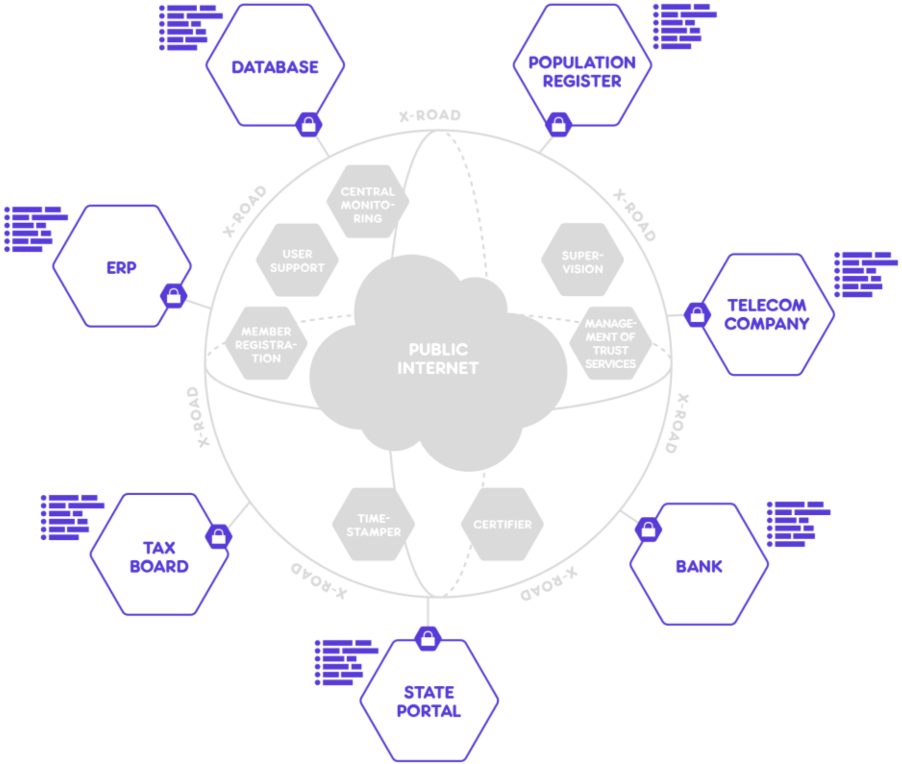
Long-term confirmation of transaction

- Timestamping messages
- Central monitoring input



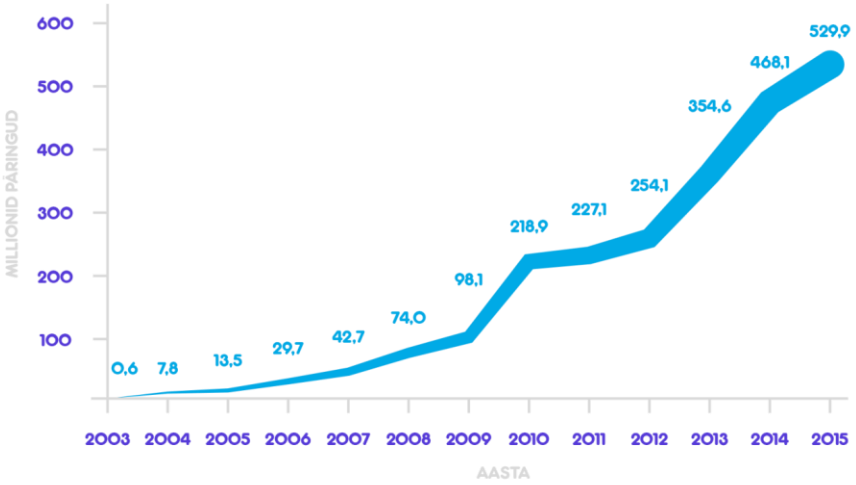
Authenticity and autonomy

- Responsibility is preserved
- Information is reliable
- Autonomy is maintained



Robust and high-quality

- 15 years of continuous operations
- Stability
- There are no back doors
- The European Framework of Interoperability
- eIDAS requirements for trust services
- Security frameworks (ISKE, ISO27001 etc)

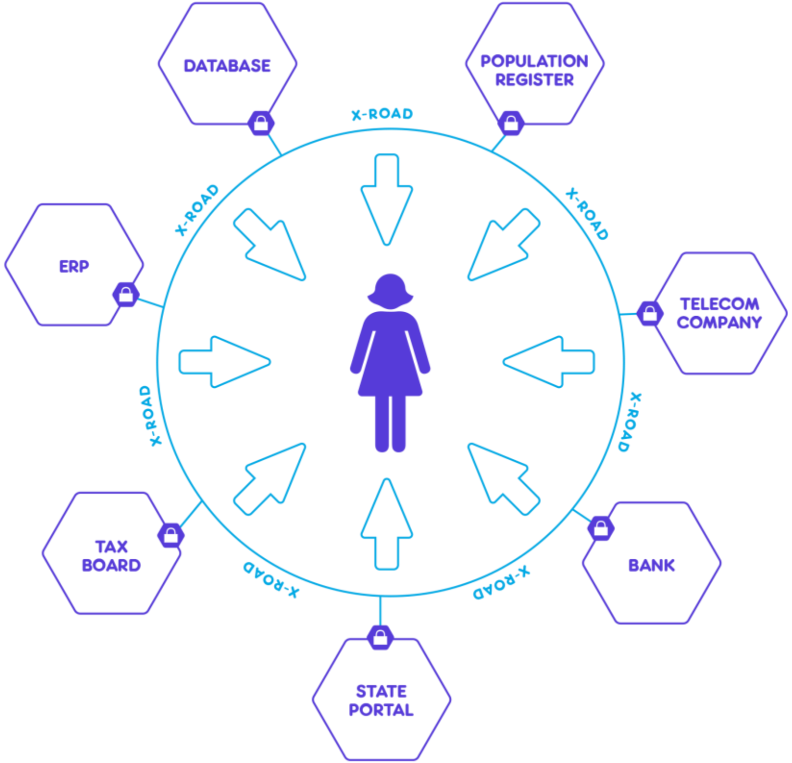


X-Road values

- Governability
- Authenticity and autonomy of members
- Security
- Flexibility
- Savings
- Robustness and quality

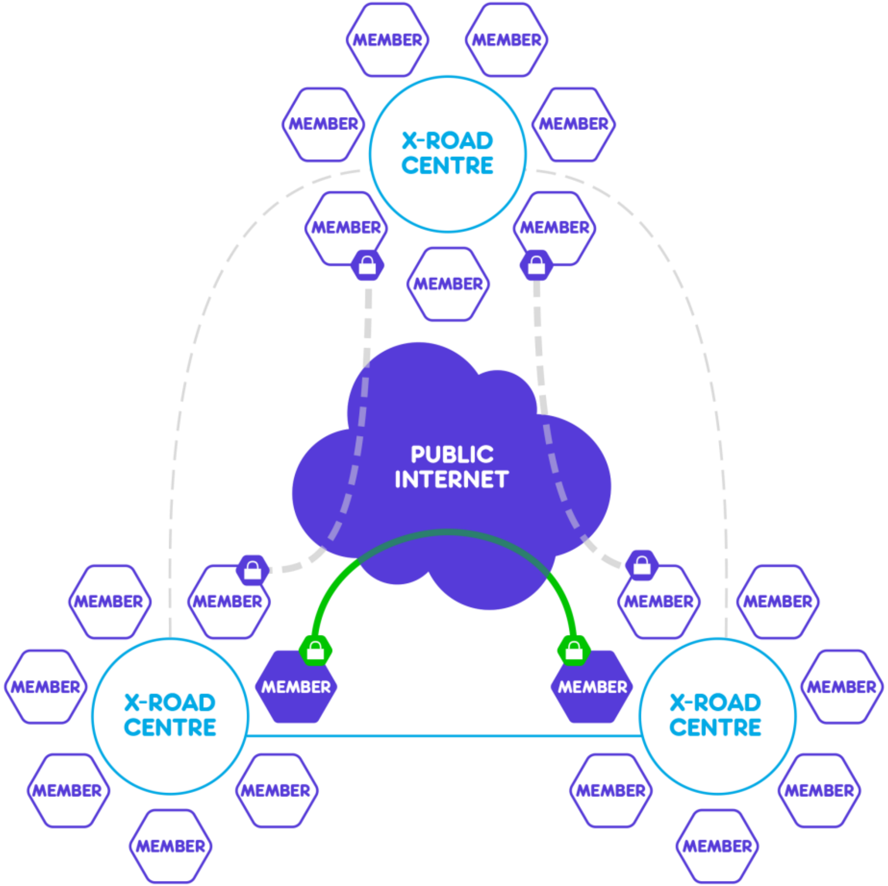
“Once-only”

Citizen must enter information only once.



Trust Federation

- Can be expanded everywhere
- Centres communicate with centres, members with other members
- Creation of cross-border services



Thank You!

Priit Parmakson
priit.parmakson@ria.ee