Secure Data Exchange Layer

Margus Püüa
E-Governance Academy, Senior Expert
Former Head of Department of State Information Systems
Agenda

• Why do we need secure data exchange?
• Architecture of secure data exchange layer
• The working principle of secure data exchange layer
What is X-Road?

• X-Road is a distributed, secure and standardized data exchange solution.
• Public and private sector organizations are welcome to use this environment.
• X-Road can be used for offering, combining and using e-services in many different fields.
Distributed exchange

Architecture before X-Road

Source: Cybernetica AS
Which problem we have to solve?

the data can not leak out

nobody can not change the data received

high availability

99,999%

High-quality public service

Source: Cybernetica AS
Architecture with security servers
X-Road Architecture

Central services:

- Certification;
- Secure service catalogue;
- Monitoring

Source: Cybernetica AS
Design goals

- X-Road is **decentralized**
- X-Road does not change **ownership of data**
- Secure
- X-Road messages are usable as **digital evidence**
- All the communications is implemented as **service calls**
- Cross-border services
- Encapsulating the security protocol
- Standardization
- No predetermined roles
- Two-level authentication

ega.ee
Main components and interfaces of the X-Road system

Deployment view of a basic X-Road instance
Main components of central server

Central Server. Simple Deployment

- Management Services
- Signer
- Web Server
- Database
- User Interface
- Servlet Engine
- Password Store

SSCD
Main components and interfaces of the X-Road security server

Database model of X-Road security server
Security Server. Simple Deployment

Security Server
- Signer
- Proxy
- Message Log
- Metadata Services
- Database
- Configuration Client
- User Interface
- Servlet Engine
- Password Store
- Operational Monitoring Buffer
- Operational Monitoring Services
- Environmental Monitoring Service
- Monitor
Confidentiality

- SSL (TSL) protocol against external attackers
- Two level access rights control
- Core X-Road: Access to organization
- Consumer organizations responsible for end users
- Balanced use of technical and organizational measures
Non-repudiation

- All outgoing messages are signed
- All incoming messages are logged and time-stamped
- Message receiver can later prove with time-stamping mechanism, when and by whom was the message sent
High availability

- Minimal number of central services
- Directory service based Secure DNS
- Time-stamping non time critical way
- Local DNS caching
- Re servers and load sharing
- Mechanisms against DoS attacks
- Availability on the same level of Internet
How the X-Road works

Service consumer organization

Internet

Service provider organization

Security server
Adapter
Database server

Security server
Application server
Security server

Central monitoring server

X-Road central servers

X-road central organization

Users

Service consumer organization

Application server

Security server
X-Road message flow

Service consumer organization
Service users
Security server of IS
Service consumer IS
Security server of DB
X-Road
Adapter
DB
Service producer (DB) organization
Trusted service provider
1. User authenticates himself/herself. Information System must be able to get to know the proper Personal Code of user.

2. Whether user is identified by ID-card, mobil ID or something else is up to the Information System, provided that the way of identification is reliable.

3. Information System gives user access to methods user is authorized to use. This is first level of authorization.

4. As user chooses to call a method (usage of which is authorized by the Information System), a message with method call goes towards the Security Server.

5. In addition to the message body with data for method call, the message contains also a message header with user’s Personal Code, the name of Information System, unique ID of the message etc.
X-Road message flow

1. The Security Server of IS signs the message with its private key.
2. The Security Server of IS asks over DNSSEC the Central Server for IP address of the Security Server(s) of DB.
4. The Security Server of DB verifies over DNSSEC the certificate received from the Security Server of IS.
5. If certificate was valid, the Security Server of DB sends its certificate back to finish creation of secure connection.
6. The Security Server of IS verifies over DNSSEC the certificate received from the Security Server of DB.
12. As secure channel has been created and other party verified, Security Server of IS sends signed and encrypted message to Security Server of DB

13. Security Server of DB verifies signature of the message and logs the message

14. Security Server of DB checks whether the Information System is authorized for this method. This is the second level of authorization

15. Security Server of DB sends the decrypted message to the Adapter Server

16. Adapter Server commits the method call in the database

X-Road message flow
17. Security Server of producer encrypt and signs the response message

18. Security Server of producer sends encrypted and signed response message to the Security Server of IS

19. Security Server of IS checks the signature of response message and logs the response message

20. Security Server of IS sends decrypted response message to the Information System

21. Finally, user receives response he/she requested!
X-Road: Trusted logs (1)

Security Server of DB logs messages coming from the Information Systems

X-Road

Security server of DB

Adapter

Service producer (DB) organization

DB

Consumer IS

Security Server of IS logs response messages coming from the Databases

Service consumer organization

Service users

Trust service Provider
Thank You!

margus.pyya@ega.ee