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

Secure Data Exchange Layer **X-Road**

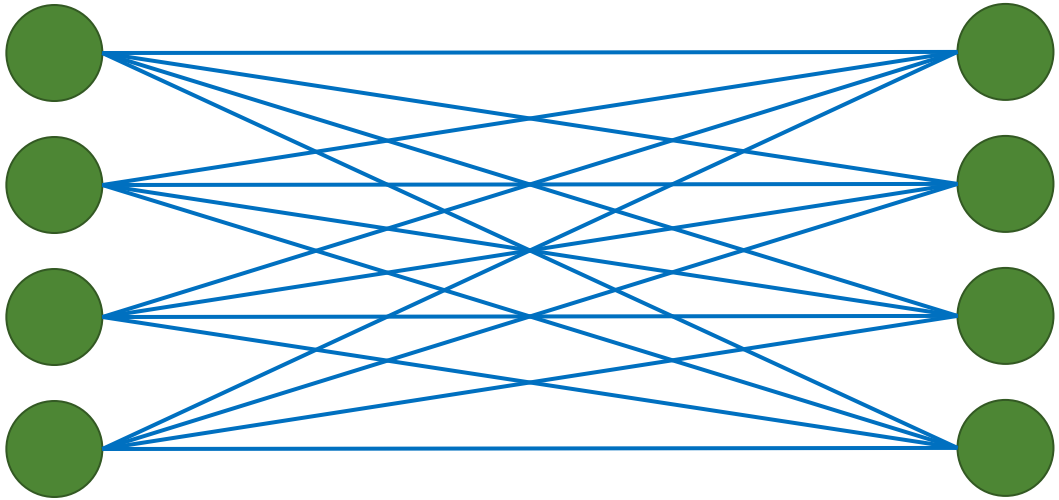
(Estonian Example)

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

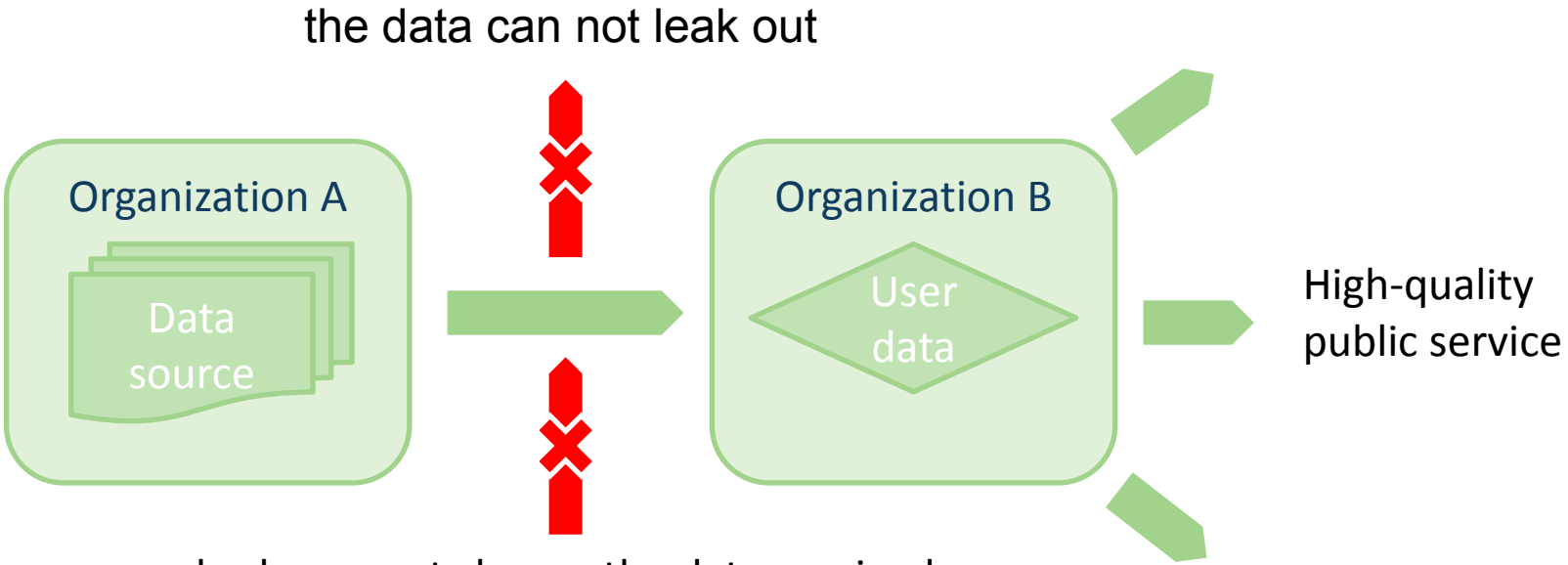
Architecture before X-Road



ega.ee

Source: Cybernetica AS

Which problem we have to solve?



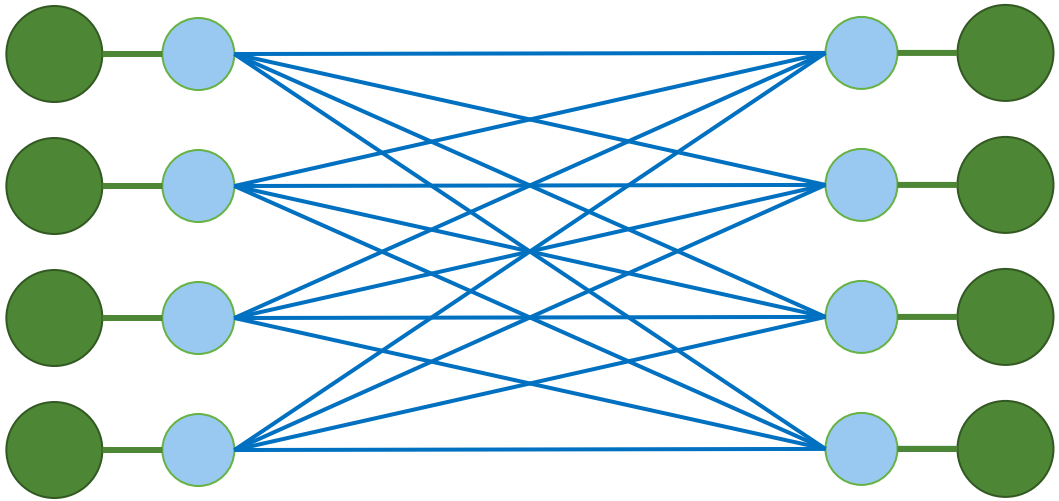
high availability

99,999%

ega.ee

Source: Cybernetica AS

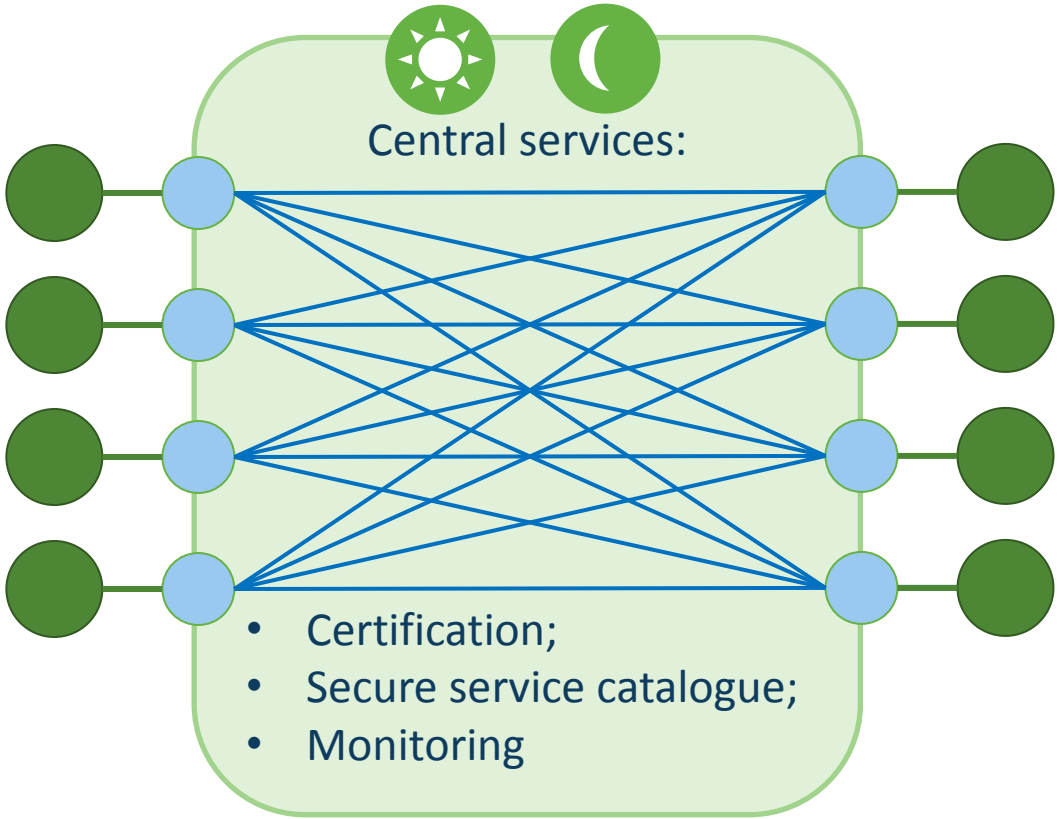
Architecture with security servers



ega.ee

Source: Cybernetica AS

X-Road Architecture



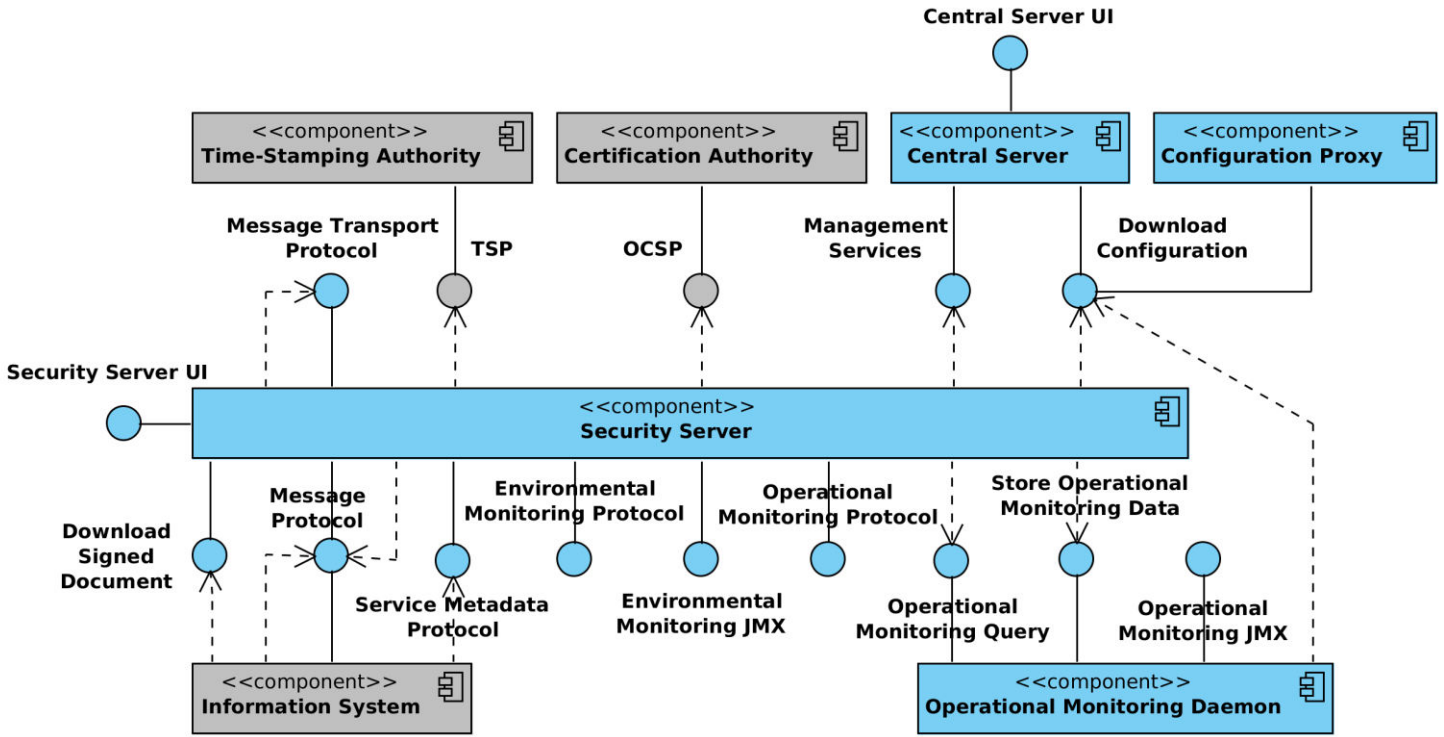
ega.ee

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**

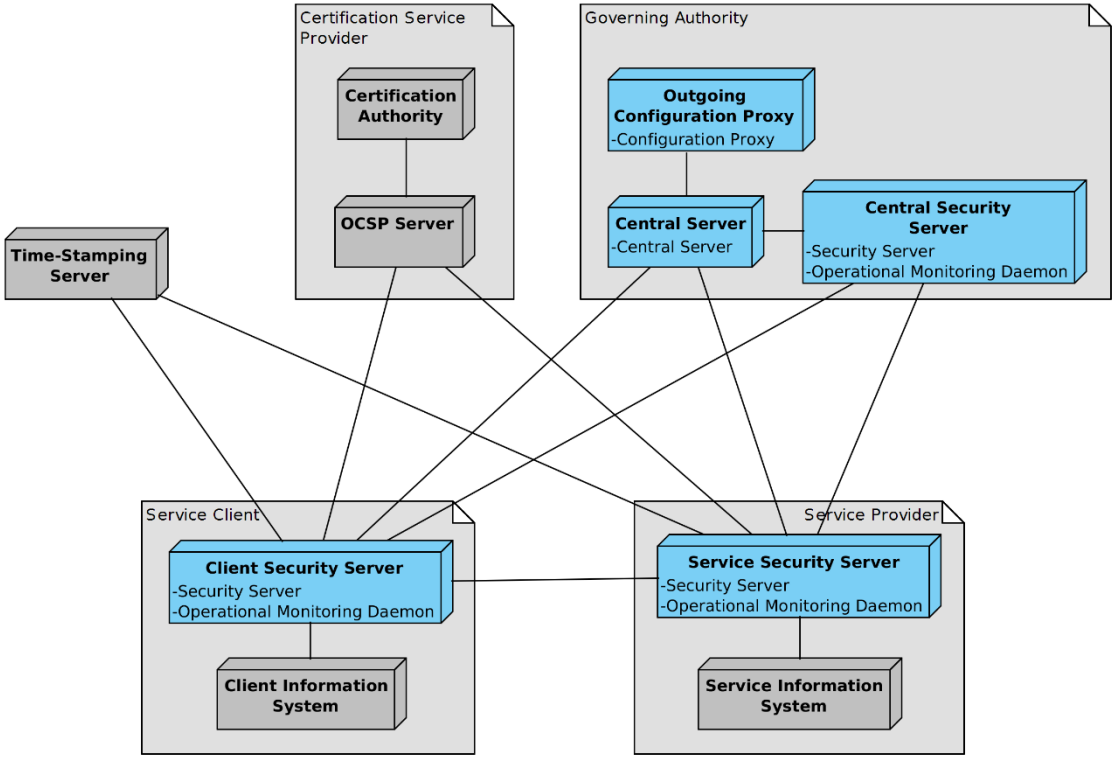
Main components and interfaces of the X-Road system



ega.ee

Sorce: X-Road Architecture Version: 1.5 20.02.2017 Doc. ID: ARC-G (https://github.com/ria-ee/X-Road/blob/develop/doc/README.md)

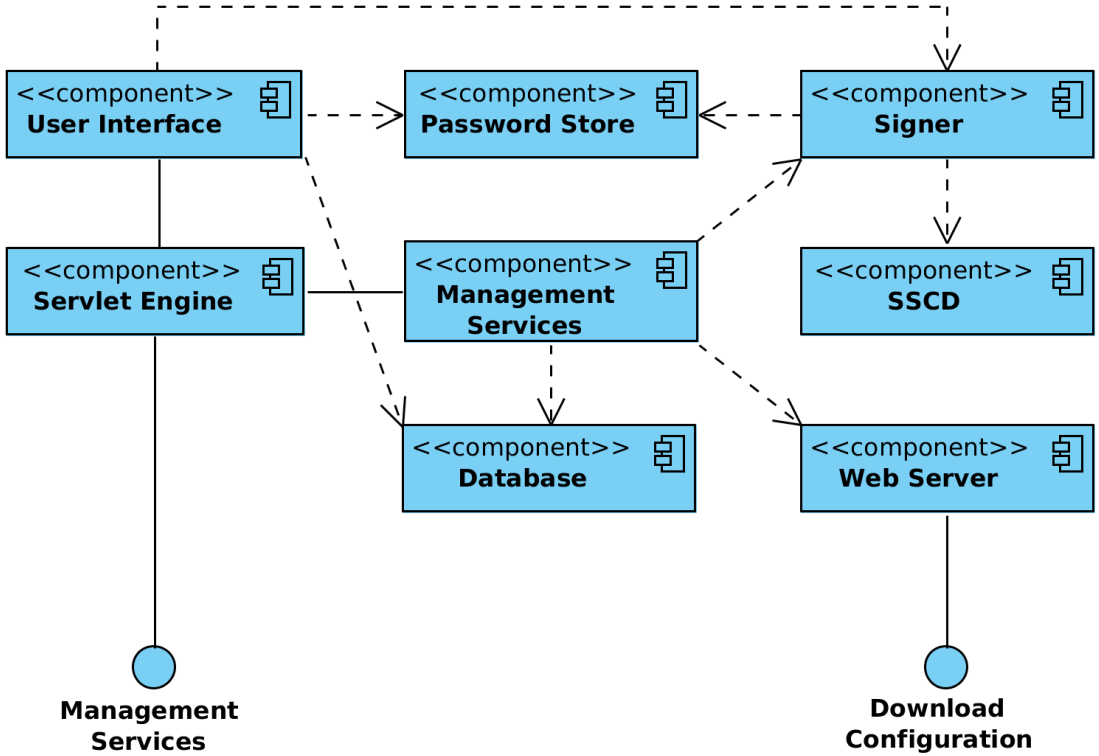
Deployment view of a basic X-Road instance



ega.ee

Sorce: X-Road Architecture Version: 1.5 20.02.2017 Doc. ID: ARC-G (https://github.com/ria-ee/X-Road/blob/develop/doc/README.md)

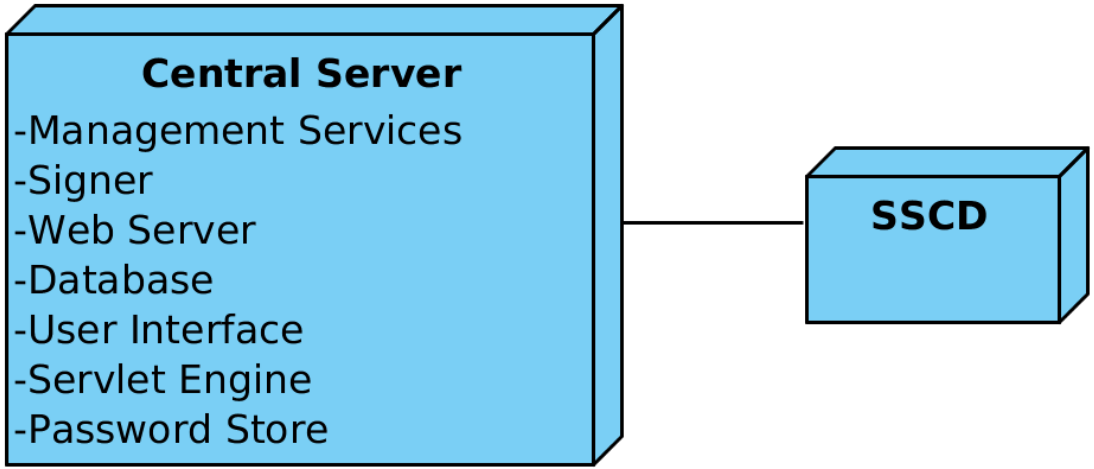
Main components of central server



ega.ee

Sorce: X-Road Architecture Version: 1.5 20.02.2017 Doc. ID: ARC-G (https://github.com/ria-ee/X-Road/blob/develop/doc/README.md)

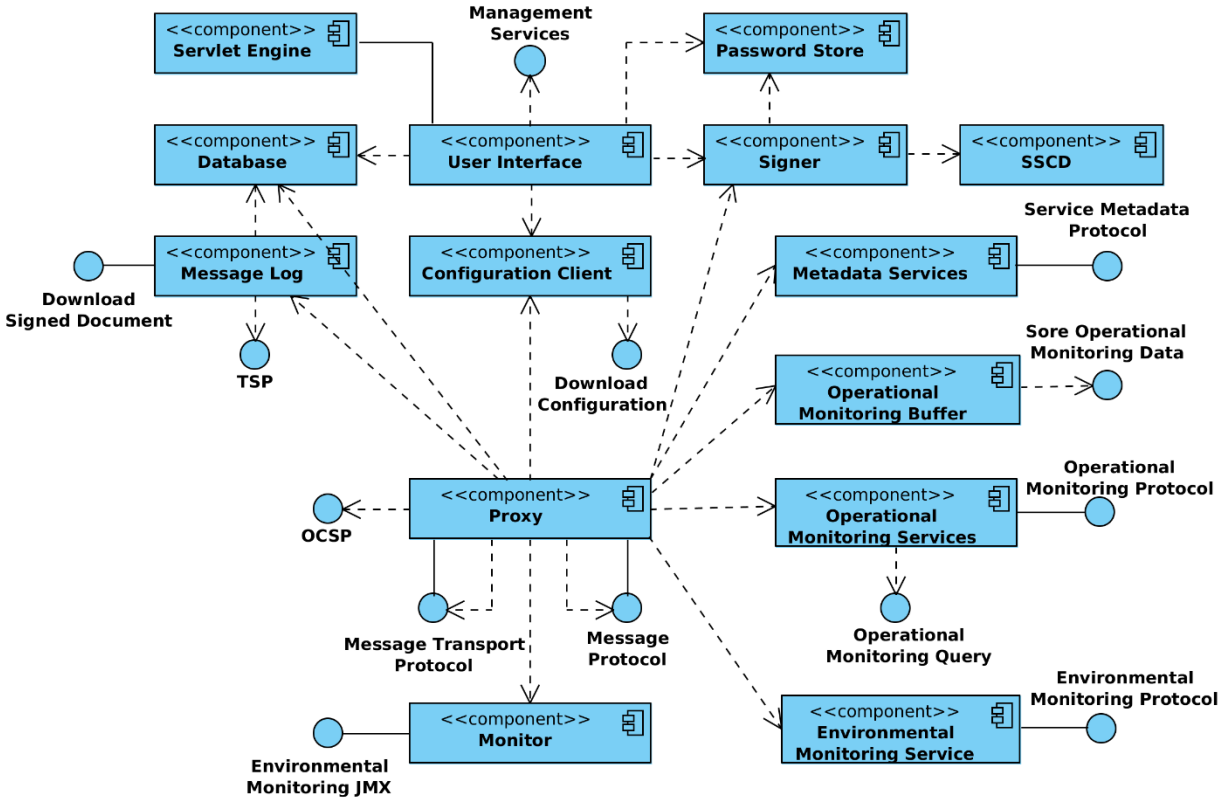
Central Server. Simple Deployment



ega.ee

Sorce: X-Road Architecture Version: 1.5 20.02.2017 Doc. ID: ARC-G (https://github.com/ria-ee/X-Road/blob/develop/doc/README.md)

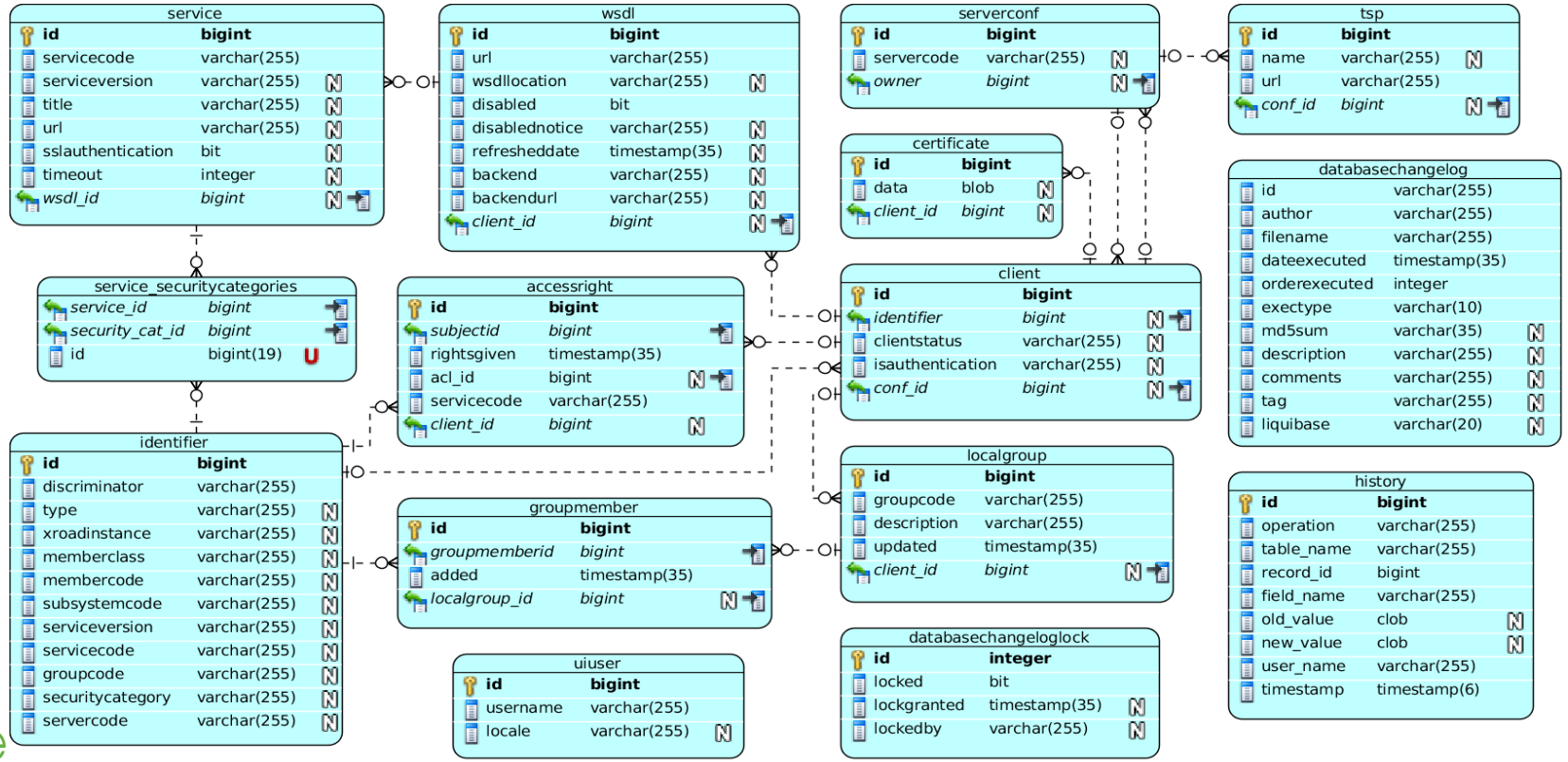
Main components and interfaces of the X-Road security server



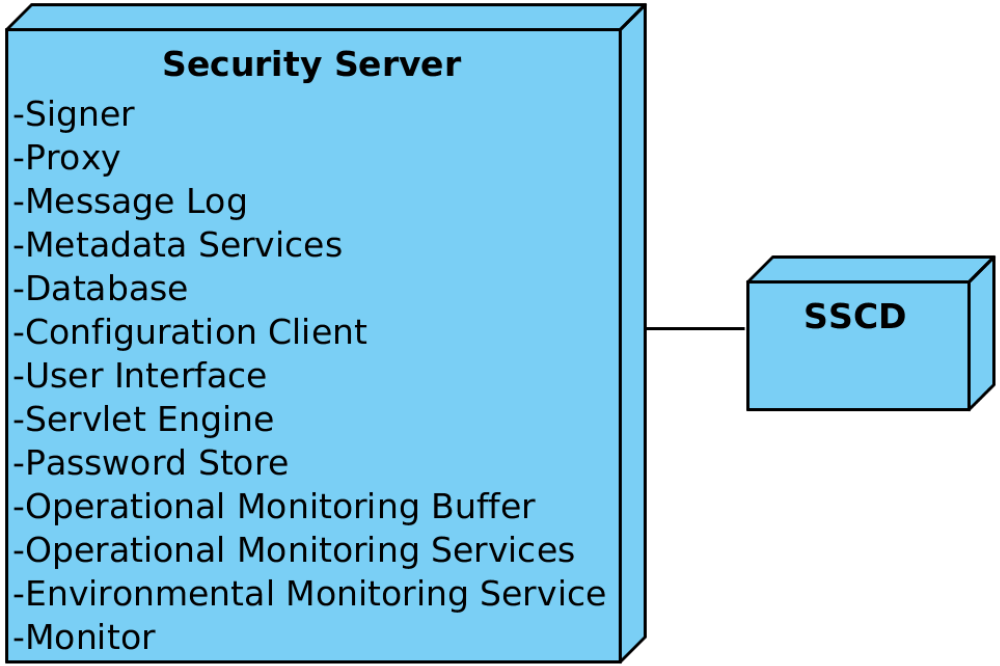
ega.ee

Sorce: X-Road Architecture Version: 1.5 20.02.2017 Doc. ID: ARC-G (https://github.com/ria-ee/X-Road/blob/develop/doc/README.md)

Database model of X-Road security server



Securiry Server. Simple Deployment



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

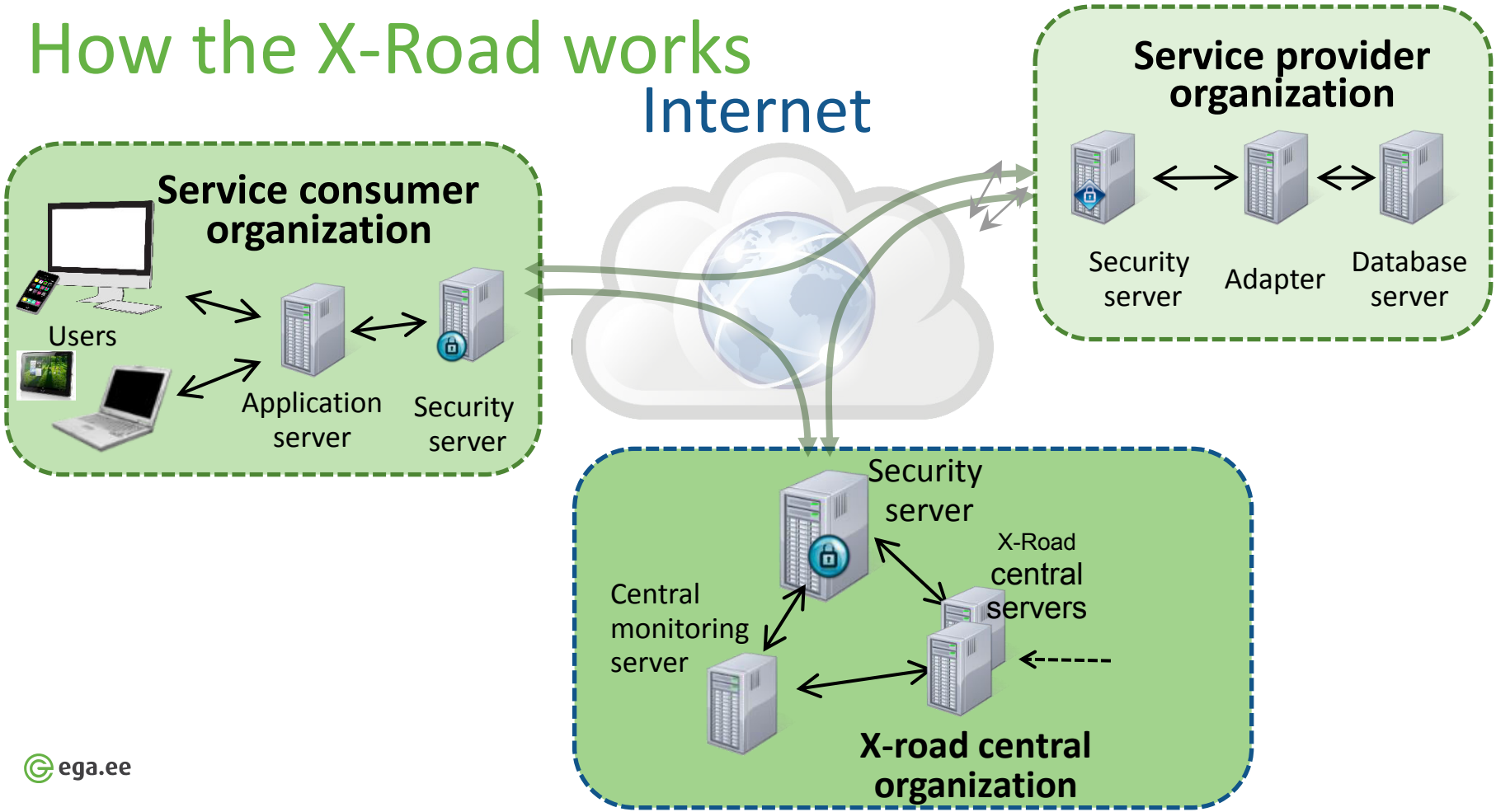
Non-repudation

- 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

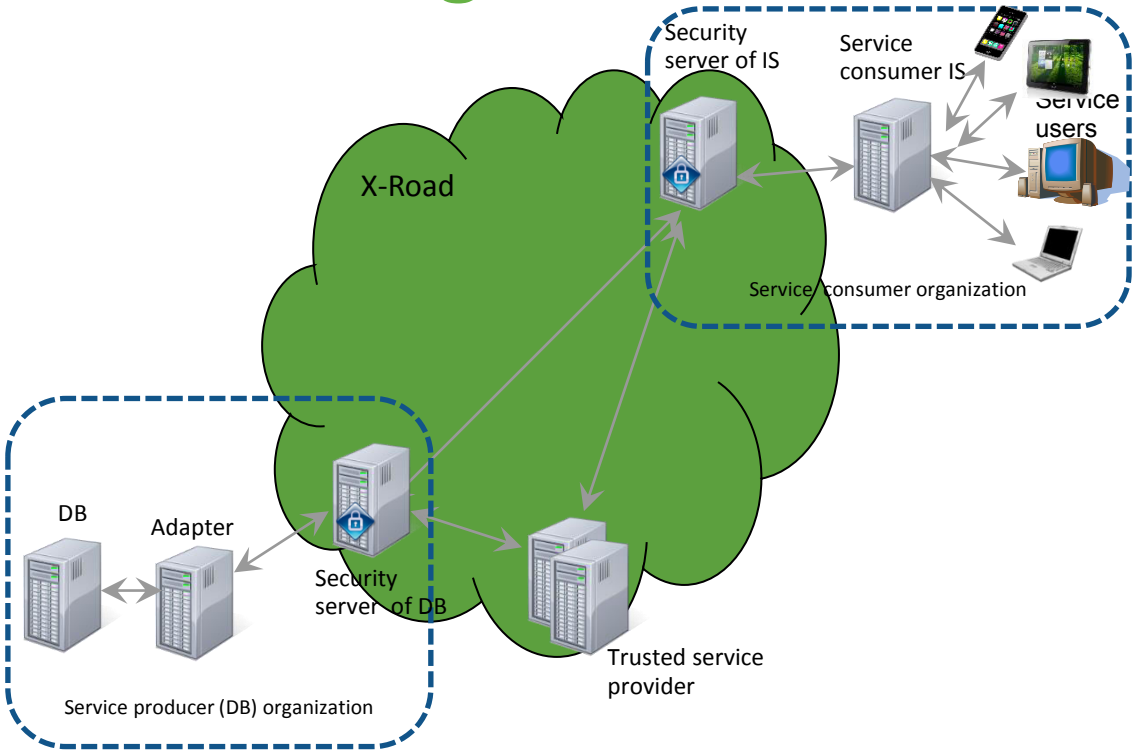
High availability

- 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

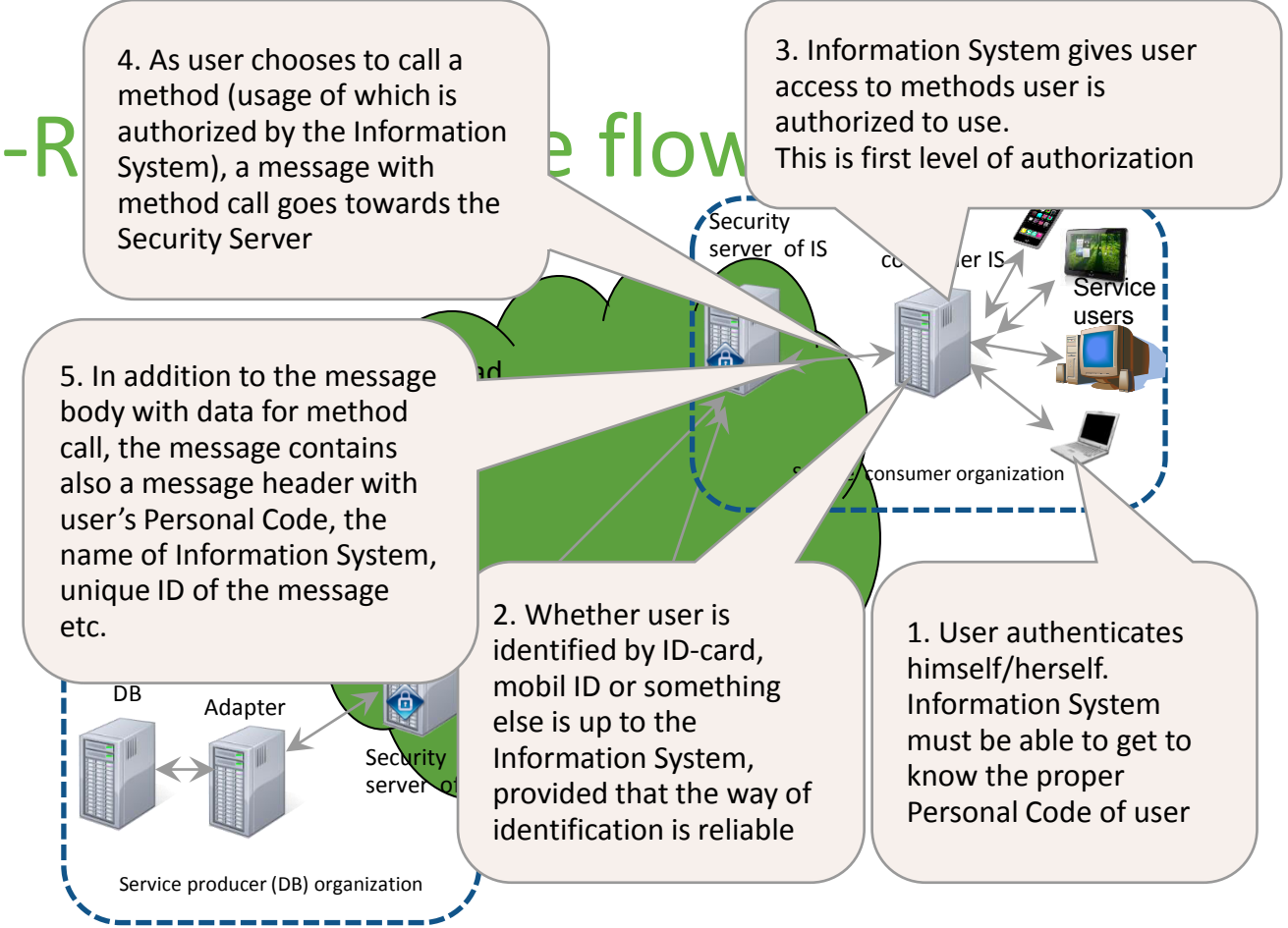


X-Road message flow

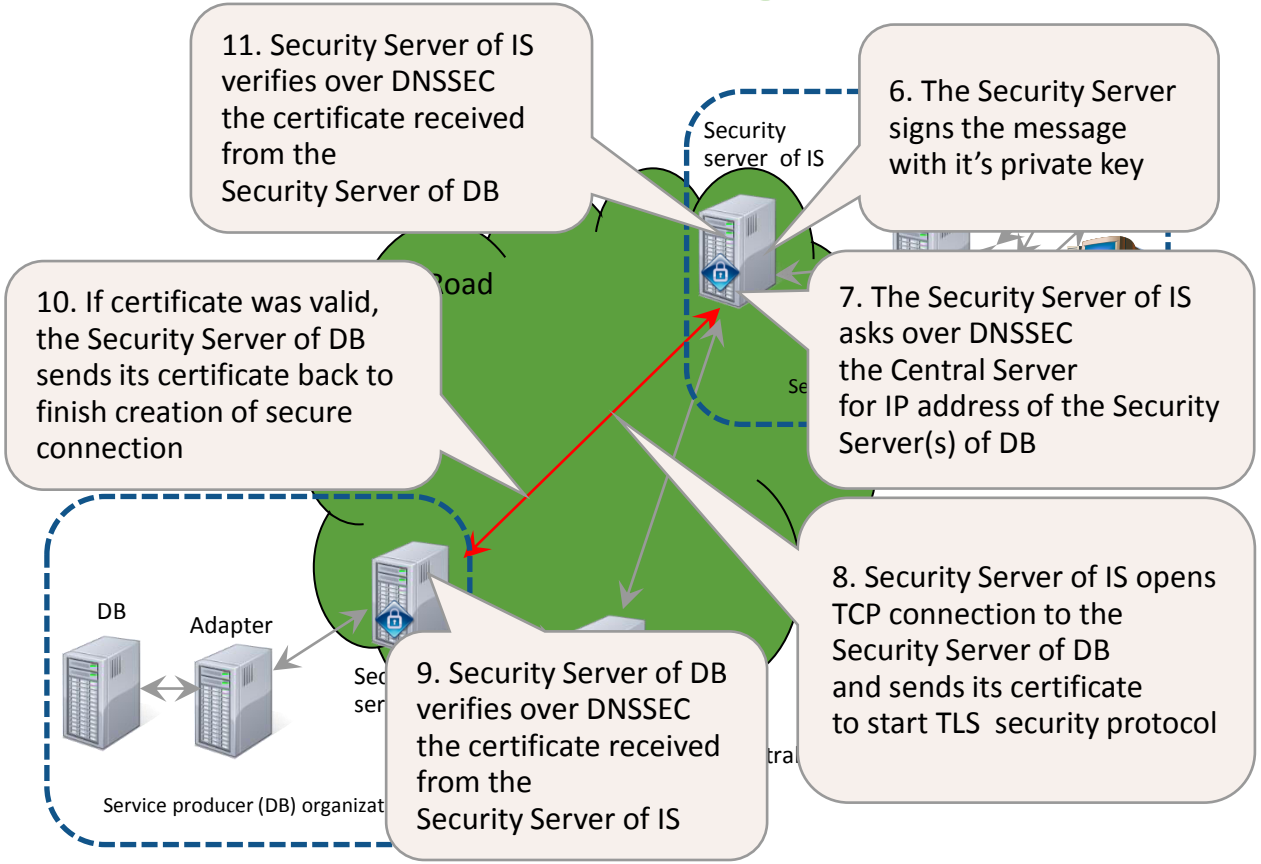


ega.ee

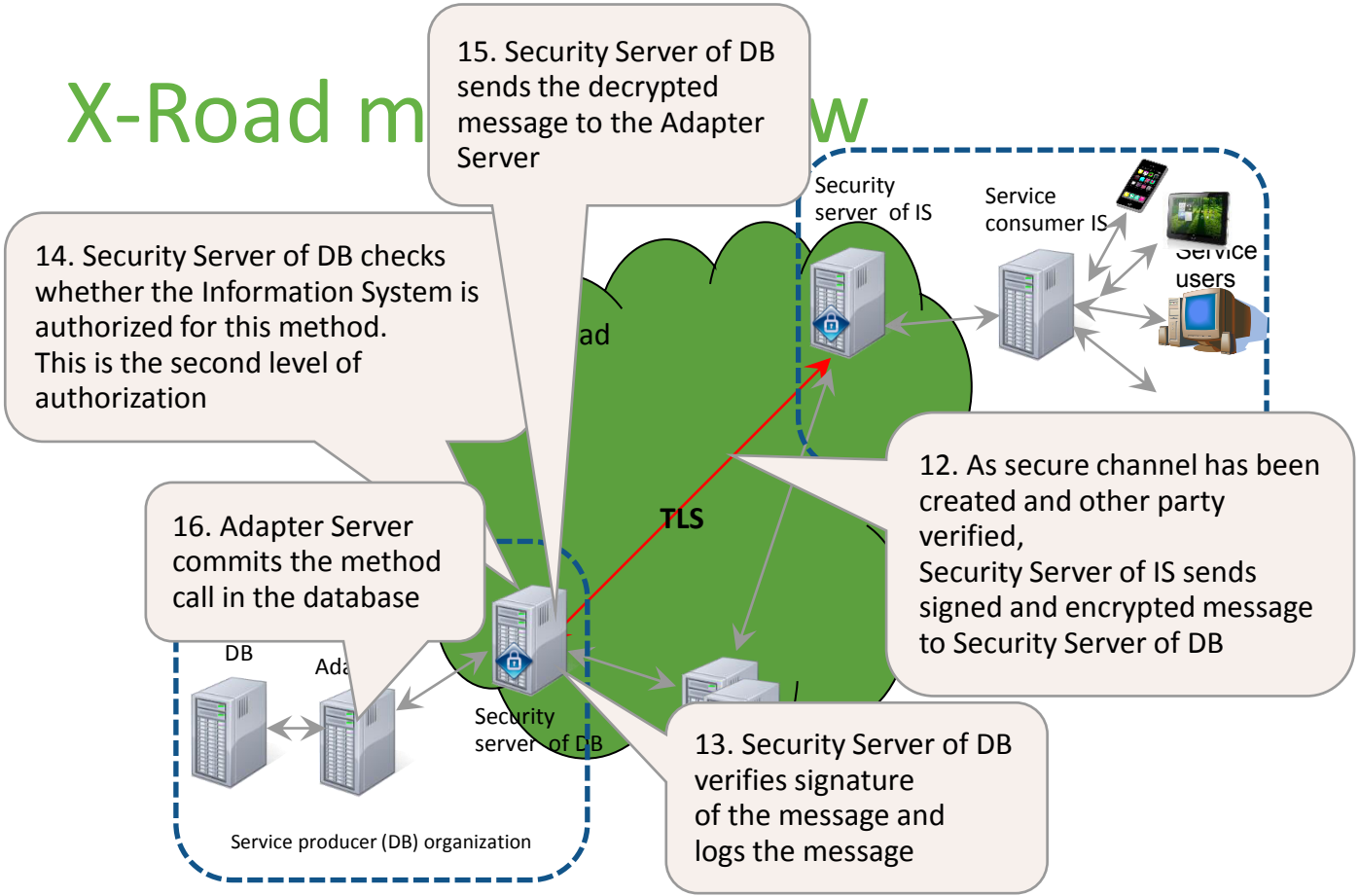
X-R e flow


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
3. Information System gives user access to methods user is authorized to use.
This is first level of authorization
Security server of IS
Service users
consumer organization
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.
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
1. User authenticates himself/herself. Information System must be able to get to know the proper Personal Code of user
DB
Adapter
Security server
Service producer (DB) organization

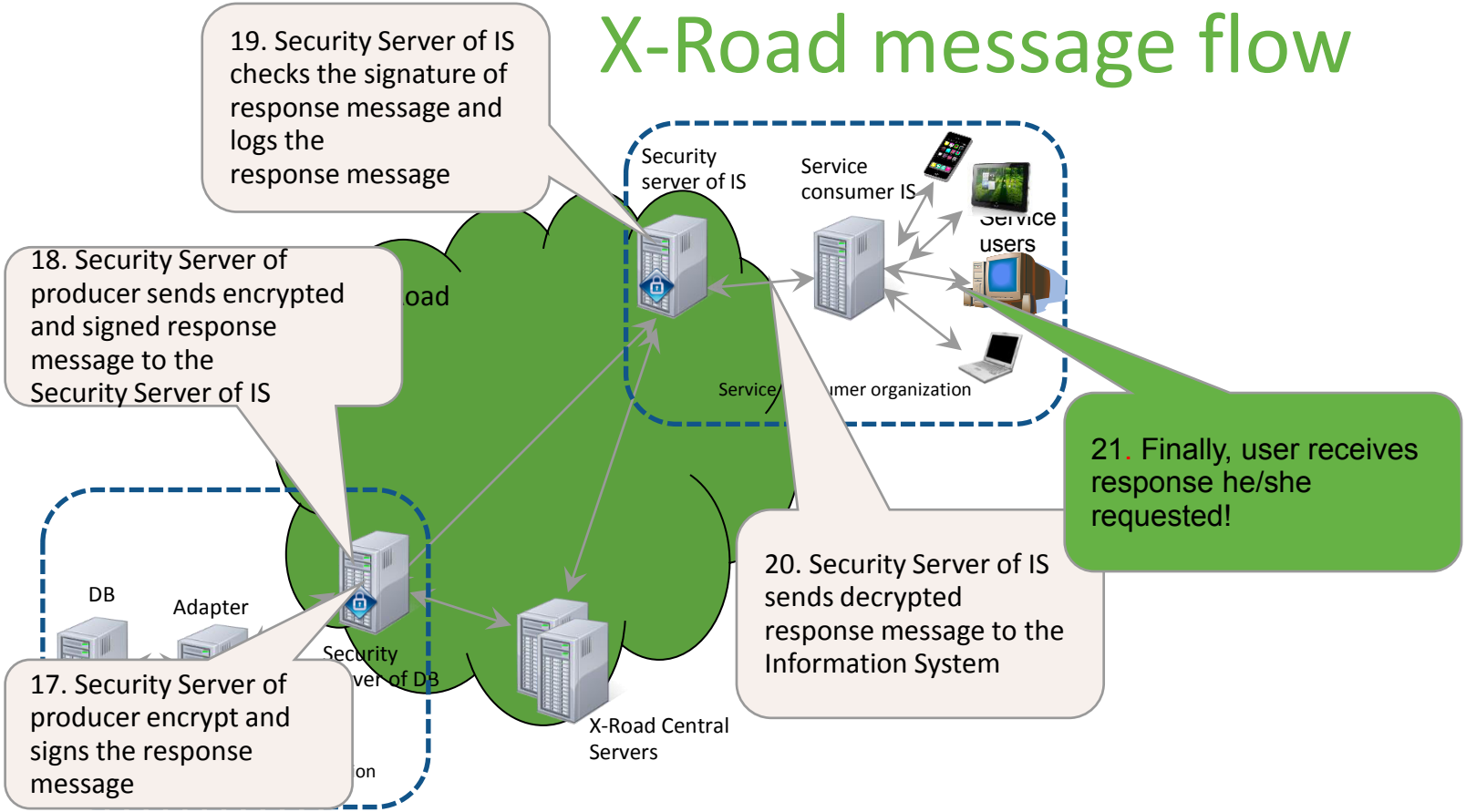
X-Road message flow



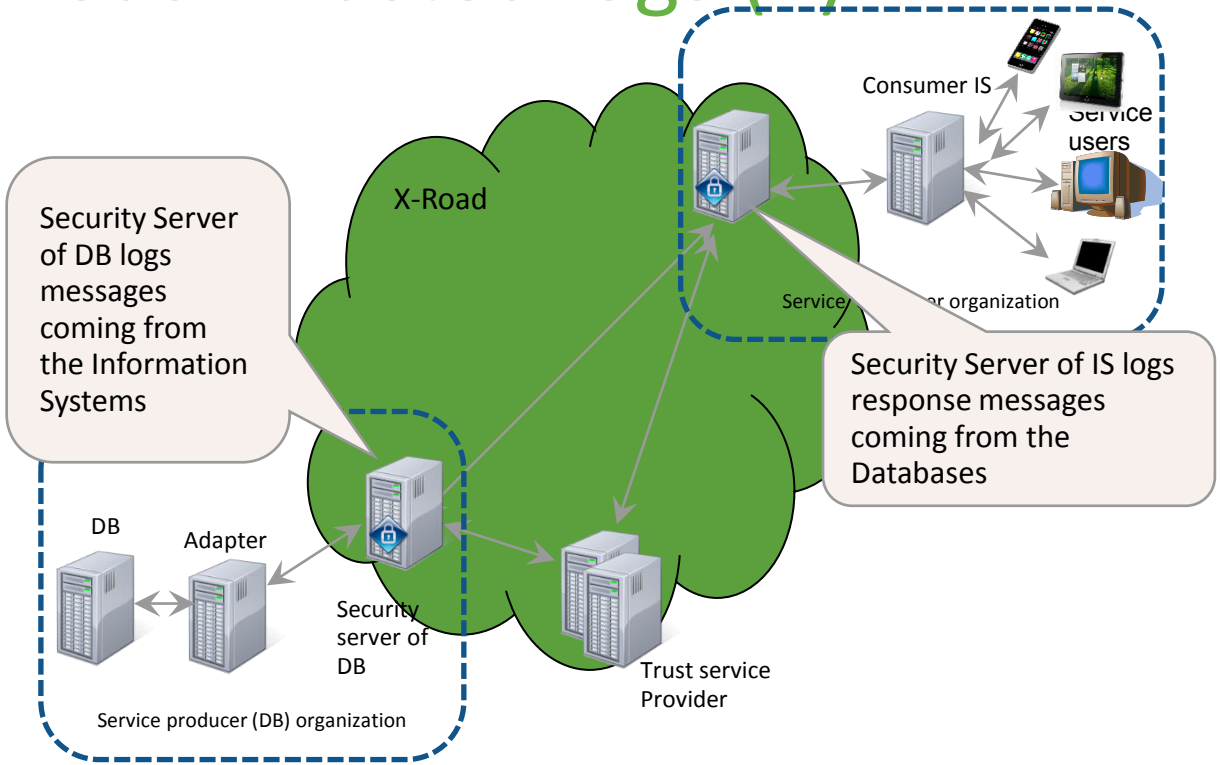
X-Road m w


15. Security Server of DB sends the decrypted message to the Adapter Server
14. Security Server of DB checks whether the Information System is authorized for this method.
This is the second level of authorization
16. Adapter Server commits the method call in the database
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
Security server of IS
Service consumer IS
Service users
TLS
DB
Security server of DB
Service producer (DB) organization

X-Road message flow



X-Road: Trusted logs (1)



Thank You!

margus.pyya@ega.ee

ega.ee