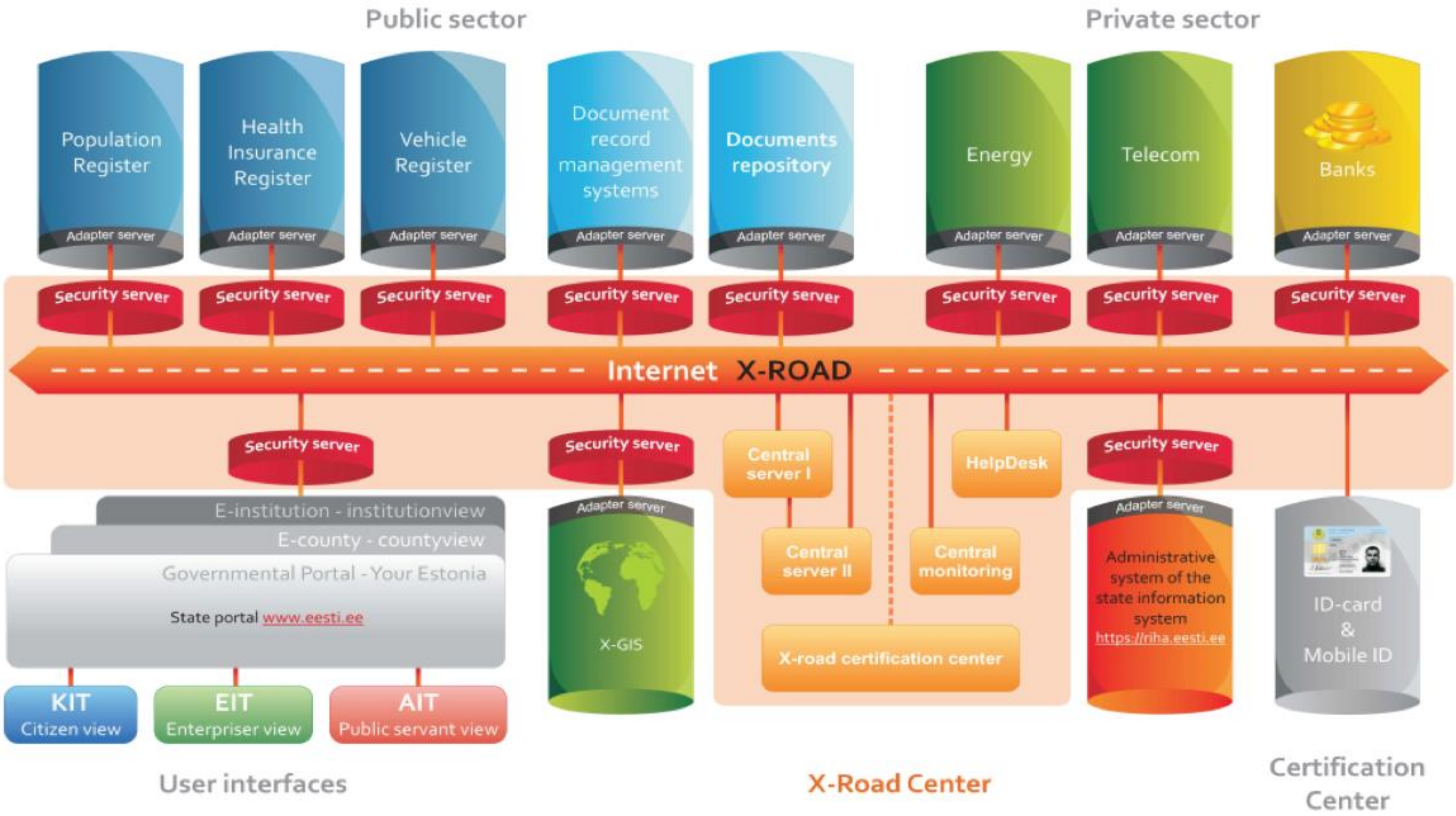
System security for data exchange

ega.ee

Margus Püüa
Senior Expert



Public sector

Private sector

Population Register

Adapter server

Security server

Health Insurance Register

Adapter server

Security server

Vehicle Register

Adapter server

Security server

Document record management systems

Adapter server

Security server

Documents repository

Adapter server

Security server

Energy

Adapter server

Security server

Telecom

Adapter server

Security server

Banks

Adapter server

Security server

Internet X-ROAD

Security server

E-institution - institutionview

E-county - countyview

Governmental Portal - Your Estonia

State portal www.eesti.ee

KIT Citizen view

EIT Enterpriser view

AIT Public servant view

User interfaces

Security server

Adapter server

X-GIS

Central server I

Central server II

Central monitoring

HelpDesk

X-road certification center

X-Road Center

Security server

Adapter server

Administrative system of the state information system https://riha.eesti.ee

ID-card & Mobile ID

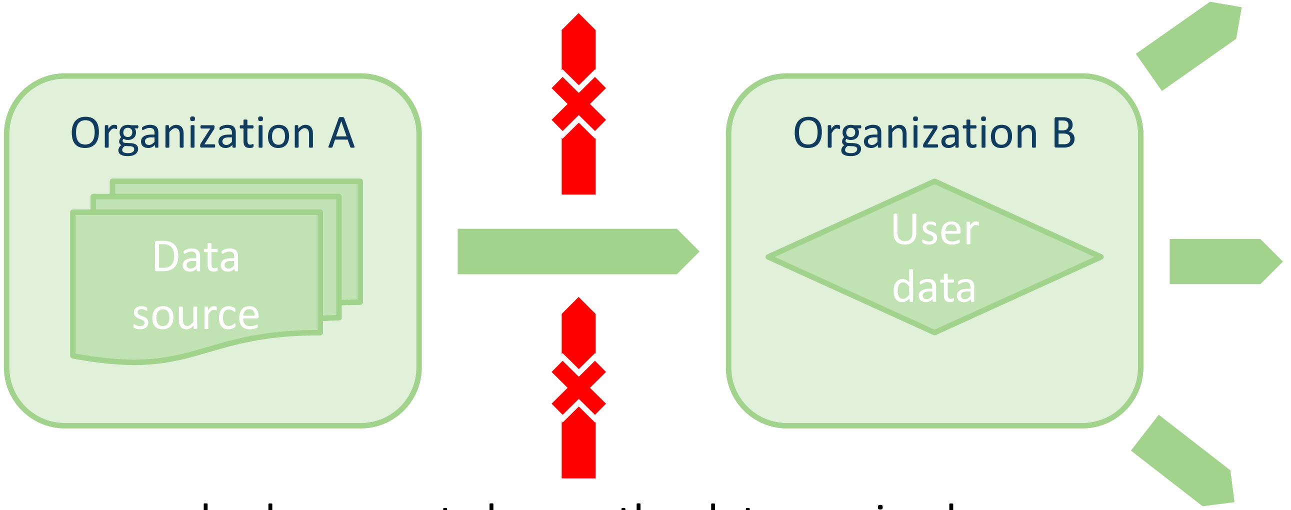
Certification Center

X-Road Secure Data Exchange Layer

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

Wich problem we have to solve?

the data can not leak out



High-quality public service

nobody can not change the data received

high availability
99,999%

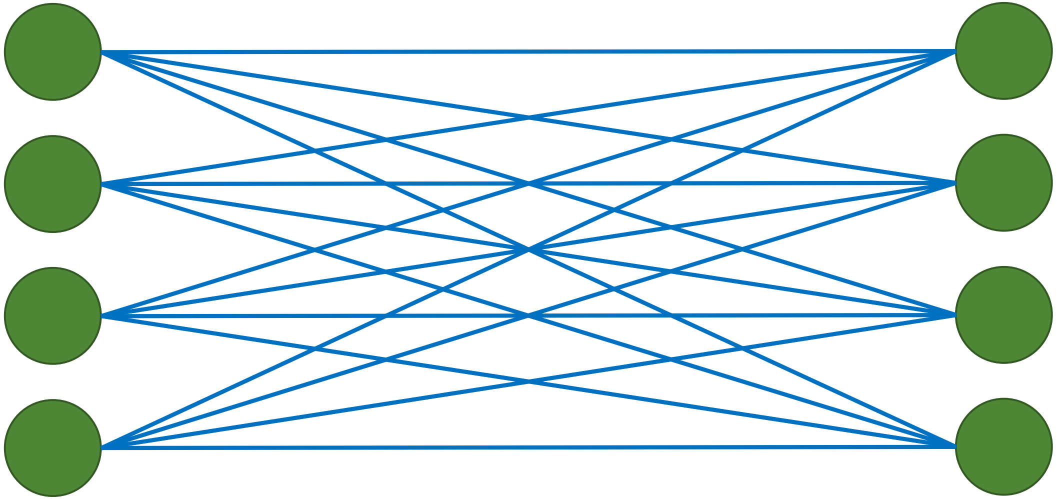
Source: Cybernetica AS

What we protect – the data or channels?

- Should we protect the king (person) or route (where king is moving)?
- We have chosen the king (data)
- Most attacks (over 80%) comes from inside
- We use public Internet, but data is encrypted and signed
- Additional channels can increase availability

Distributed exchange

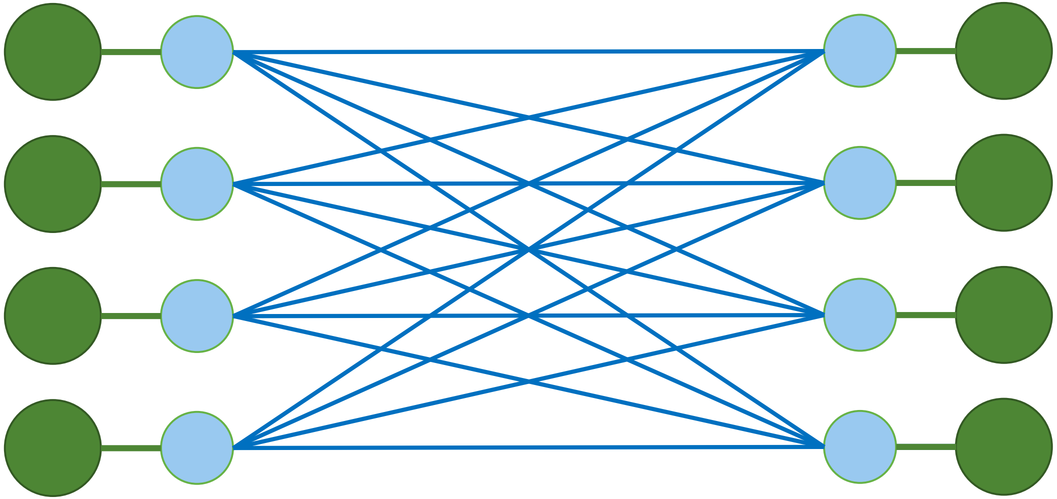
Architecture before X-Road



ega.ee

Source: Cybernetica AS

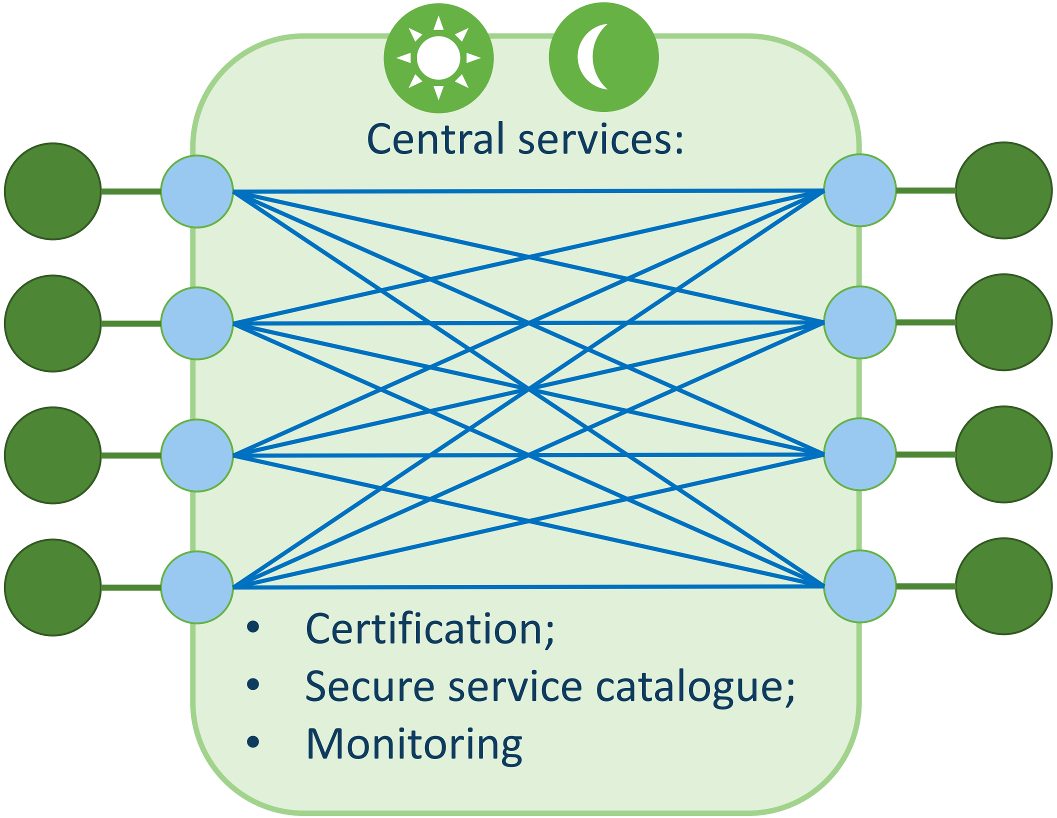
Architecture with security servers



ega.ee

Source: Cybernetica AS

X-Road Architecture

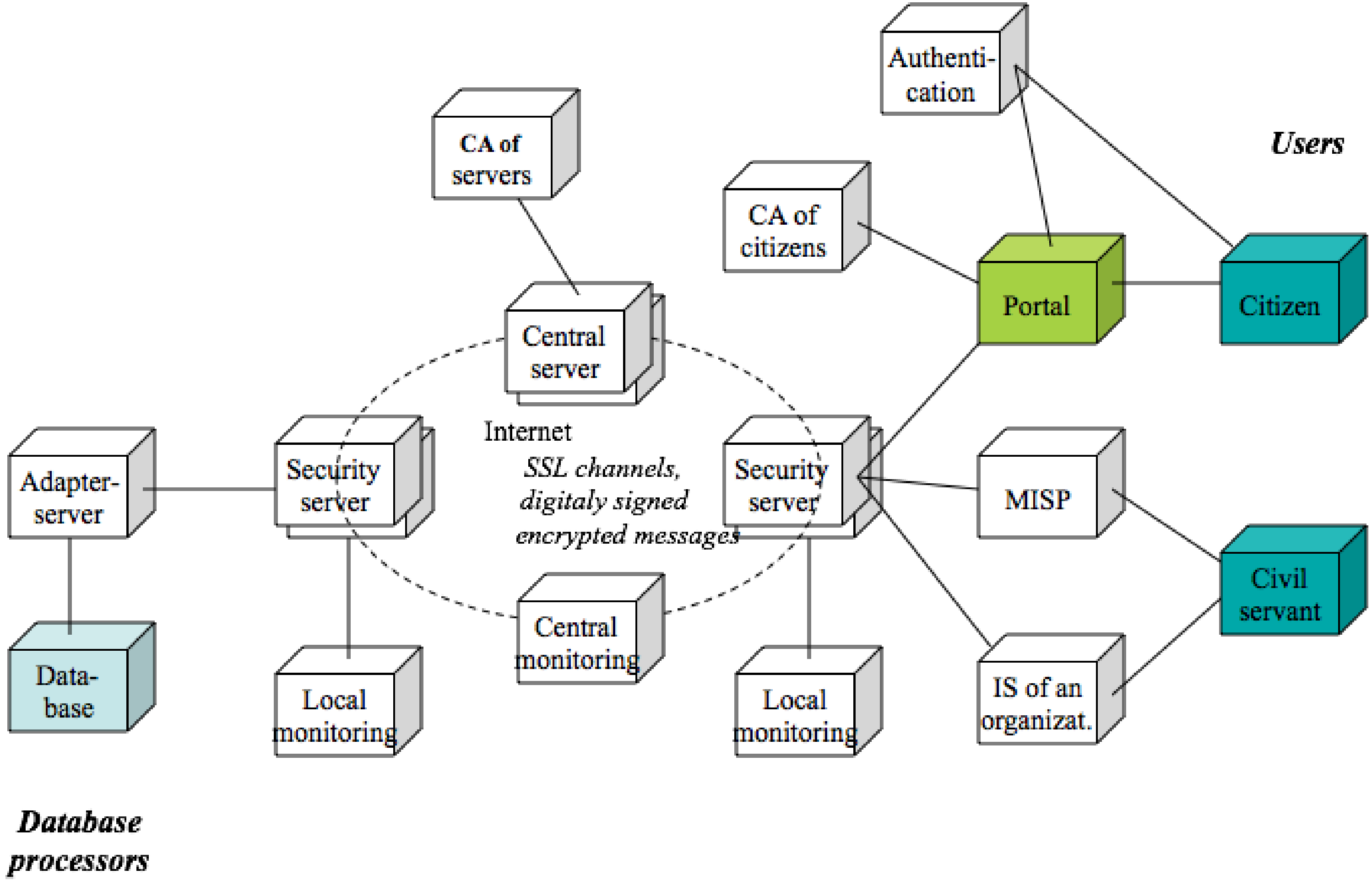


Central services:

- Certification;
- Secure service catalogue;
- Monitoring

ega.ee

Source: Cybernetica AS



Authenti-cation

Users

CA of servers

CA of citizens

Portal

Citizen

Central server

Internet

SSL channels, digitaly signed encrypted messages

Adapter-server

Security server

Security server

MISP

Civil servant

Data-base

Local monitoring

Central monitoring

Local monitoring

IS of an organizat.

Database processors

Functional scheme

Central server

Central server provides information about the X-road users´ certificates and IP addresses.

Central server has the following tasks:

- DNSSEC – resolving providers´ IP addresses and publishing x-road consumers´ /producers´ certificates;
- Provides DNSSEC public key for initial download over HTTP;
- Distributes information about central monitoring servers;
- Distributes certificates from CA server;
- NTP-SERVER – keeping security servers´ time in sync;
- Storing all hashes of secure logs from security servers.

Certification Authority server

- CA server is an offline server;
- X.509 certificates to security servers
  - For authenticating each other
  - For digital signatures of queries and responses
- The database of the X-road users´ certificates and IP addresses is managed by CA server
- Offline service using Hardware Security Module (HSM) for secure key storage
- Certificates and IP addresses are exported to Central Server, using offline media (USB flash drive).

Central monitoring server

- Monitoring stations provide x-road security - and central servers status information to system administrators;
- Receives periodical information about status of all security servers and all central servers (CPU, memory, disk, version…);
- Monitoring Station is also collecting service usage information (message envelope headers);
- Usage information contains only META-DATA (query time, user ID, user organization ID, database name and service name).

Security server

Security server is dedicated proxy server for exchanging data between service consumers and providers.

Security server's assignment is to:

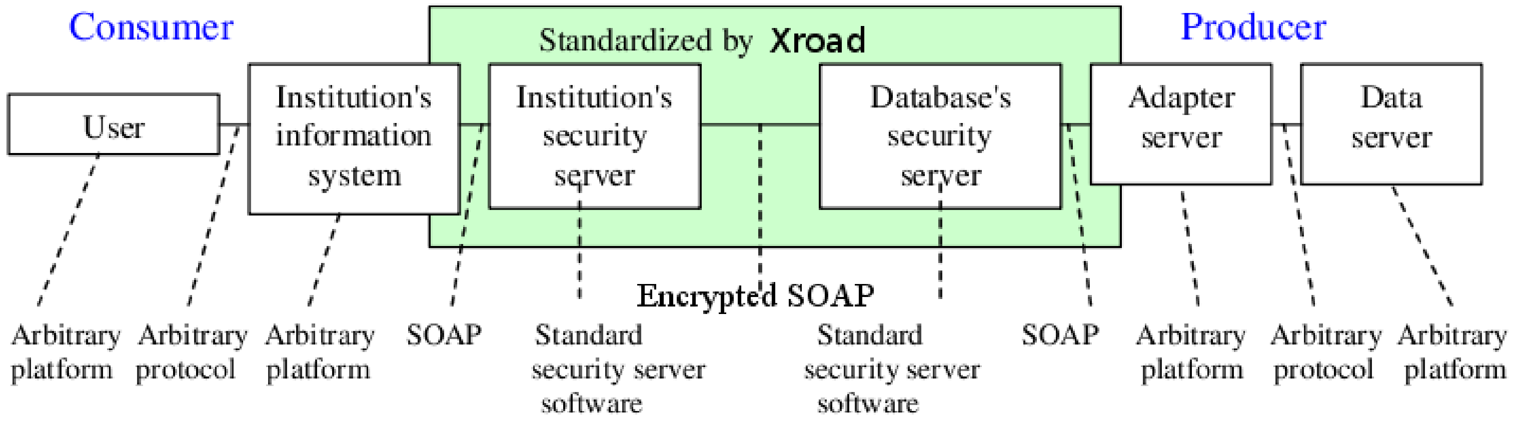
- Forward queries to a right producer/consumer over TLS secure channel;
- Check if consumer's/producer's certificate is valid;
- Encrypt/decrypt data (like a TLS SOAP VPN ☺);
- Check if consumer has permission to access services (ACL list);
- Log queries (request/response to ‘sslog’);
- Saves secure log hashes periodically to central servers.

Local monitoring server

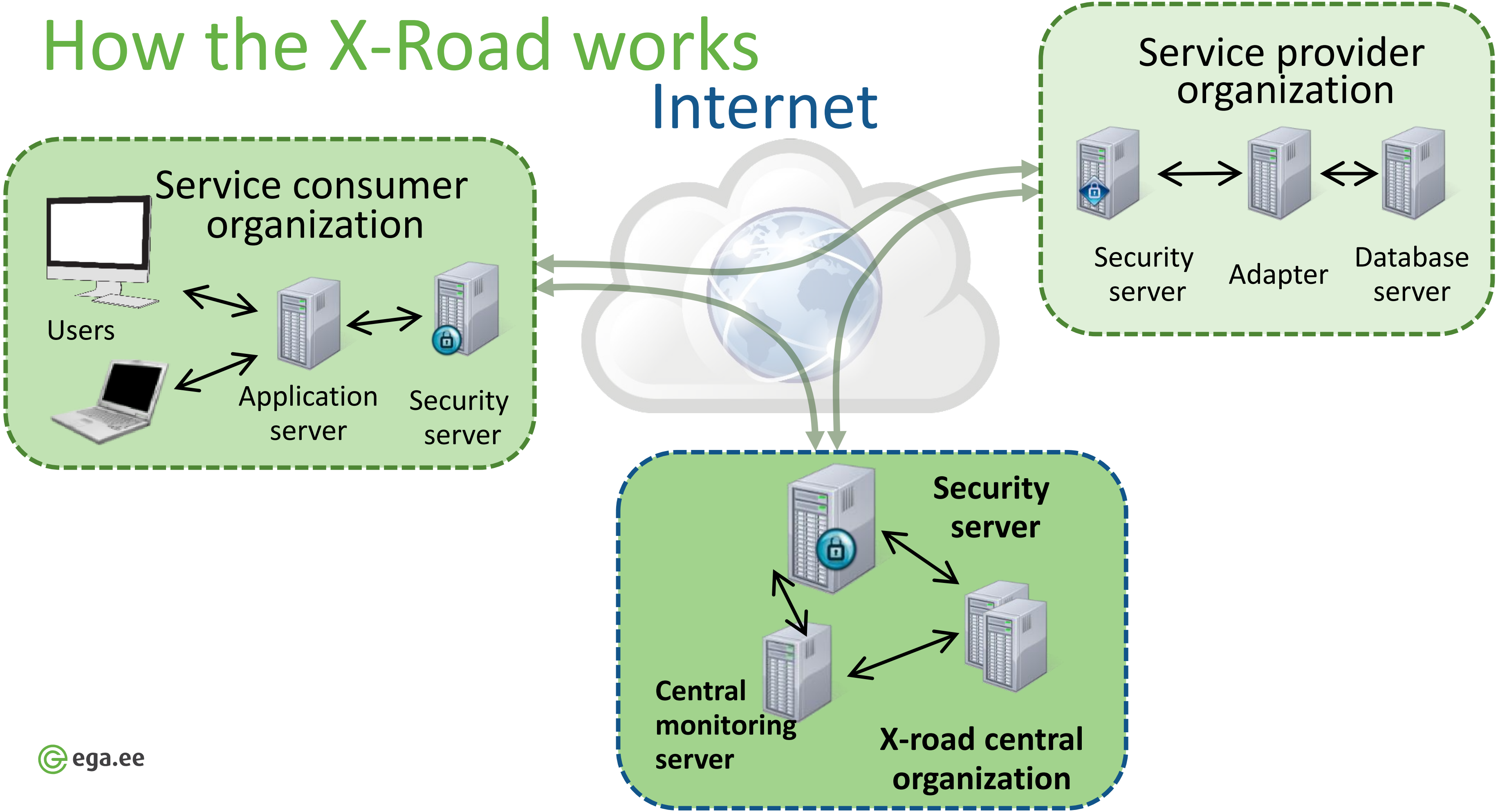
- Local monitoring servers are installed locally aside to some security servers
- They receive the same information, but only from some security servers that are explicitly configured to send a copy there
- Provides the same analysis as central monitoring servers, but for local admins only

Adapter server

is a web service provider which modifies the x-road queries to a specific format of a database platform.



How the X-Road works


Internet
Service consumer organization
Users
Application server
Security server
Service provider organization
Security server
Adapter
Database server
Security server
Central monitoring server
X-road central organization

ega.ee

Thank You!

margus.pyya@ega.ee

ega.ee