Secure data exchange platform. Principles and implementation. X-Road

2017-12-12

Table of Contents

1. Introduction

Current document gives the overviews and detail technical specifications and standards how to create interconnection and exchange information between different distributed autonomous e-government applications.

The documentation will decrease the effort, time and cost required to develop the electronic exchange of data between government agencies for securing interoperability. Using those standards and technical specifications, government agencies can set up and maintain the information sharing with other agencies by themselves.

The technical approach is based on the experience from the similar projects worldwide. Detail specifications and standards are tested in real governmental environments in different countries and based on the working interoperability solution X-Road.

Technical part of the current document starts with section 2, covering the architectural principles needed to implement the true e-Government. Presented key architectural principle is single data collection ("once-only principle"). This principle means, that information must be supplied to information consumers only once from the source responsible for the handling this information and there is no other information source for the same information.

Second main architectural principle is that for true e-services, full society must act as a service centred organization. It means that all the activities of officials, entrepreneurs, citizens and software/information system are viewed as services.

The main criteria for the interoperability solution are described in the section 3 of this document. In addition, the assessments of the different interoperability solutions are presented.

The technical specification section (section 4) gives overview of the interoperability solution X-Road. It includes full documentation of the different components. Those descriptions are extremely practical as those are taken from the proved and working interoperability solution X-Road Estonia. Full specification, including source code, you can find in X-Road github: https://github.com/ria-ee/X-Road. You can find learning material from https://moodle.ria.ee/. Many useful materials and guides you can also find from https://www.roksnet.com/.

X-Road is developed in Estonia and implemented in many countries e.g. Finland, Azerbaidzan, Ukraine, Argentina, Namibia, Haiti, Faraoe Island.

This document is prepared by Uuno Vallner, e-mail: Uuno.Vallner@ega.ee

2. Architectural specification

2.1. Introduction

The architectural specifications will focus especially on concepts how to make interconnection of the existing database and exchange information between different distributed autonomous e-government applications. The goal is to decrease the effort, time and cost required to develop the electronic exchange of data between government agencies for securing interoperability.

The key concept of agreed approach is single data collection (once-only) principle. This principle means, that the current project will ensure that information is supplied to information consumers only once from the source responsible for the handling this information and there is no other information source for the same information. According to the "Once-Only" principle, public bodies should take action to share data with each other, respecting privacy and data protection rules. This calls for a generic and scalable solution to interconnect different systems.

In the next section is described conceptual model of interoperability for the planning, development, operation and maintenance of data sharing processes and integrated public services. The model highlights the need for modular, loosely coupled infrastructure components interconnected through a shared infrastructure.

The model handles society as a service centred organization, which means that all the activities of officials, entrepreneurs, citizens and software/information system are viewed as services. End users see services from a joint service room. They are not interested in the organization that provides a service but in the service itself. Although the private and public sector act according to different business rules, the users of their services are the same. Hence, it is practical if the private and public sector develop and manage the service room jointly.

In public sector information systems, front-end and back-end systems should be clearly separated architecturally. 'Back-end systems' are considered all public sectors' registers and databases. The task of back-end systems is data management and the provision of network services; they do not deal with authentication and authorization. Hence, there is no need to build into back-end systems components of end user's authentication and authorization. Web services of back-end systems are made available for the end user only through service intermediaries (front-end systems).

2.2. Conceptual model

Component-based service model for public administrations allows the establishment of Public Services by reusing, as much as possible, of existing service components. Public administrations should agree on a common scheme to interconnect loosely coupled components and put in place the necessary infrastructure. Model is based on the experiences with interoperability frameworks of Estonia, Europe[1] and other countries.

[1] European Interoperability Framework (EIF) https://ec.europa.eu/isa2/eif

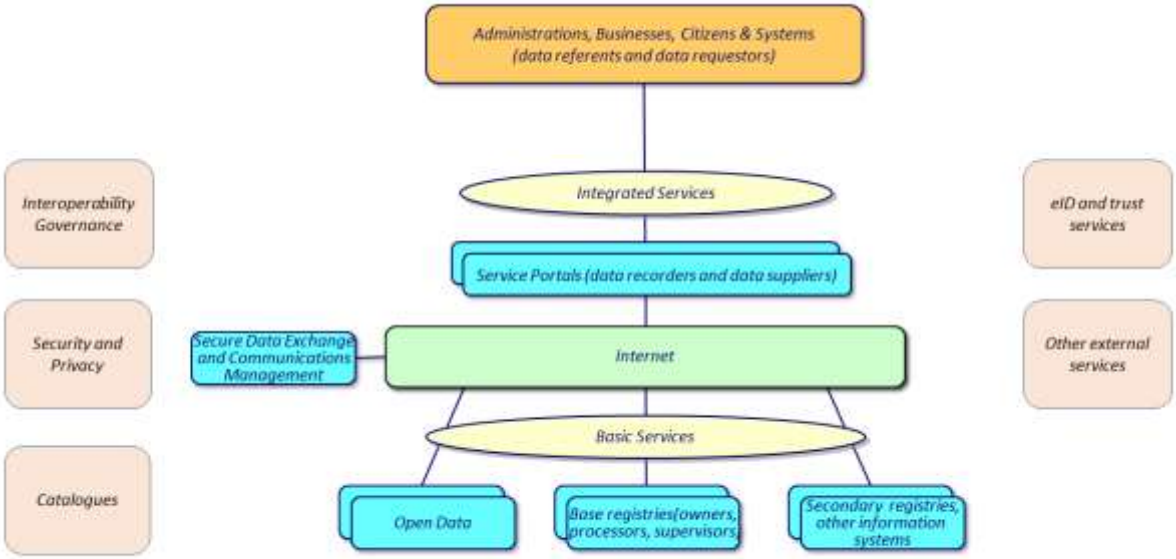

Figure 1. Conceptual model

Base registries (BR). A base registry is identified as being a trusted and authoritative source of information, which can and should be digitally reused by others and in which one organisation is responsible and accountable for the collection, usage, updating and preservation of information.

Catalogues (CA). Catalogues describe reusable services and other assets to increase their findability and usage. This component allows publishers to document and make available resources with the potential to be reused by others. Various types of catalogue exist, for example directories of services, libraries of software components, open data portals, registry of registries, metadata catalogues and catalogues of standards.

eID and Trust Services (TS). Infrastructure for identification, signing, encryption, sealing, timestamping, certificates validation

External information and services. Public administrations should exploit services provided outside the boundaries of public administrations by third parties such as, payment services provided by financial institutions or connectivity services provided by telecommunications providers.

Front end Systems (FE). Portals for supplying integrated services. Over the FE data referents and data requestors interact with different registries

Interoperability Governance (IG). Interoperability governance refers to decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability bodies responsible for e-governance strategy, coordination and implementation. Also bodies responsible for privacy and security.

Other registries (OR). A secondary registry can contain own master data and master data from base registers transferred over Secure Data Exchange layer. Actors of OR are data controllers, data

processors, supervisors. From consumer point of view, there is no difference between BR and OR. OR contains data transferred over secure data exchange component from BR

Secure Data Exchange (SDE). SDE aim is to ensure that all data exchanges are done in a secure and controlled way. This component is most crucial factor for implementation this model.

Service discovery will be implemented by web-based applications (portals) through the secure data exchange platform. Portal creates dynamic query/input forms for service consuming. The infrastructure implies the existence of state, departmental and regional portals of public services. The portal component will set up to allow citizens to access governmental e-services. Portals should support building complex (aggregated) services. Portals will support different authentication methods, based on national system of e-identification. Citizens can use computers and mobile devices to access and use these services. Number of portals is unlimited.

Security is a primary concern in the Data Sharing and in the provision of public services. Public administrations providing public services should ensure:

- that the complete infrastructure and building blocks are secure by complying with the principles of a privacy by design approach;
- that the services are not vulnerable to attacks which might interrupt their operation, cause data theft or data damage;
- and that they are compliant with the legal requirements and obligations regarding data protection and privacy.

Data sharing mechanisms should facilitate information exchanges between administrations, businesses and citizens that are:

- Registered and verified — both sender and receiver have been identified and authenticated through agreed procedures and mechanisms;
- Encrypted — the confidentiality of the exchanged data is ensured;
- Timestamped — maintain accurate time;
- Logged — electronic records are logged and archived to ensure a legal audit trail.

The logical view of the secure service infrastructure components of the Government Data Sharing Platform and their interconnection is illustrated in figure 2

The secure data exchange is based on TCP/IP networks. There are two types of members of information systems: service providers (publishers, back end) and consumers (subscribers, front end). An information system can act in both roles at the same time – publish its own data and at the same time consume data published by someone else. The number of members is unlimited. The components of the platform are displayed in figure 2 within the red box.

The most important component of the platform is the gateway. The gateway encapsulates all of the security complexity for the members of the data sharing system. Gateways standardize processes of message transfer between the members of the data sharing system. Only the sender and the receiver can see the structure and the content of the messages.

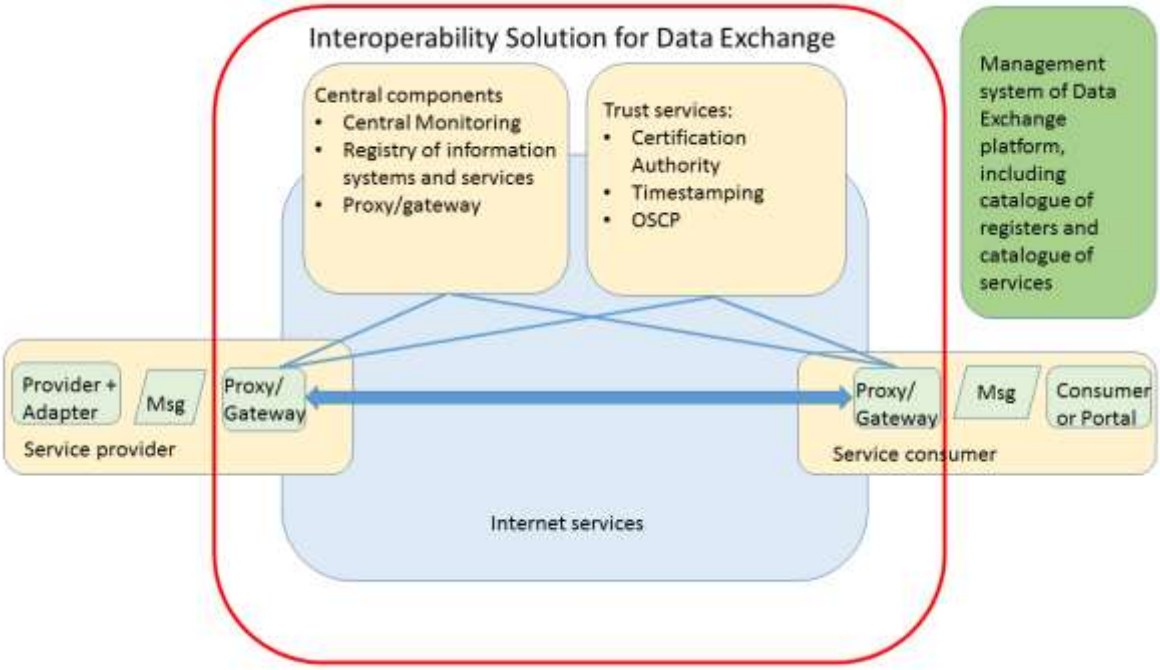

Figure 2 Secure data exchange infrastructure components

The model implies only a minimal amount of central services: registry of information systems and services, 3rd party identification and authentication, transaction log, services health monitoring and PKI functionality. Central components provide information to proxy servers about the data exchanged by participants.

These kinds of mechanisms should allow for the secure exchange of electronically verified messages, records, forms and other kinds of information between the different systems. In addition to transporting data, this layer should also handle specific security requirements such as electronic signatures creation and verification, encryption and time stamping. Furthermore, there should be monitoring of traffic to detect intrusions, changes of data and of other type of attacks.

The provision of secure (i.e. signed, verified, encrypted and logged) data exchange via Data exchange platform requires several management functions, including:

- Service management to oversee all communications on identification, authentication, authorisation, data transport, etc., including access authorisations, revocation and audit;
- Service registration to provide (subject to proper authorisation) access to available services through prior localisation and verification that the service is trustworthy;
- Service logging to ensure that all data exchanges are logged for future evidence and archived when necessary.

3. Requirement specifications for data exchange platforms

3.1. Methodology

If country has chosen decentralised model, each ministry or Government organization maintains its own certified open data registries, and authentic base registries. Ministries, agencies and businesses, if certified, may re-use these unique registries to create one-stop services for administrations, businesses and citizens. The data sharing platform transfers SOAP or REST (or other) legally certified messages between interoperating systems, i.e. between Open Data registries, Base Registries, External Services, and One Stop Service Portals. The chosen platform SHOULD provide for 'agnostic' message transfer, i.e. the platform does NOT have any knowledge of the message structure (syntax) or message content (semantics), NOR of inter-organizational process management. Message syntax, standardization, semantics and processing are the responsibility of interoperating ministries and agencies (and certified businesses).

In this section, we evaluate how different data exchange platforms comply with the requirements set to the interoperability solutions. The comparison of different platforms, used worldwide, is done by using the methodology of Michiel Malotaux2, based on global eGovernment best practice. The four popular governmental data sharing platforms: GovTalk (examples of implementations: UK, Georgia, Serbia), WSO2 (Moldova), X-Road (Estonia, Azerbaijan, Finland, Namibia, Haiti, Faroe Islands, Kyrgyzstan, Palestine, Tunisia), Info Highway (Singapur, Mauritius). Values of WSO2 and X-Road are taken from study of independent expert Michiel Malotaux. GovTalk and Info Highway assessment is added in this study.

We use five-stage approach to indicate the maturity of the criterion in a specific solution:

Score	Maturity stage	Interpretation
1	Ad Hoc	Poor fulfilment. Almost the criterion is not met
2	Opportunistic	Fair fulfilment. Some elements of best practices appear
3	Essential	The essential best practices appear
4	Sustainable	Major best practices are implemented
5	Seamless	Leading example

The criteria 4.2-4.6 measure the score of a platform for governance agency and its connecting organisations ("value criteria"). The criteria 4.7-4.14 indicate the suitability of platform if implemented, operated and maintained by the governance agency ("feasibility criteria").

3.2. Message transfer

The "Message transfer" criterion considers how the exchange of information messages between connecting ministries, agencies and other organizations is enabled. "Message transfer" is concerned with security and non-repudiation (certified dispatch and certified receipt), not with the message content. "Agnostic message transfer" means that the interoperability solution transfers the bits/bytes of the message, without any knowledge of the structure and/or content of the message.

[2] Michiel Malotaux. eGovernment Interoperability Solution. The Vision Labs. 9 May 2016.

In some solutions, all messages are sent from the provider platform to a central portal which transfers the message to the consumer platform. This causes the central portal to become a single point of failure and a performance bottleneck (all the messages exchanged HAVE to pass through this portal, therefor this portal has to accommodate increasing traffic as Info Highway gains more ground). The system administrator of central platform can read the message transfer log, which contains real data and which means that the administrator can see the exact information exchanged between two parties

Evaluation score of current criteria: GovTalk - 4, WSO2 - 4, X-Road – 4, Higway - 3

3.3. Trust

The “trust” criterion is being considered to evaluate trust between connected organizations. Trust is mandatory between different organizations (that may not even know each other). Trust is established by the following security facilities:

- Identification – to identify an entity (a person or a system) sending and/or receiving messages
- Authentication – to ascertain that an entity really is who it claims to be
- Certification – to certify (sign) a message sent, or a message received
- Encryption – to ensure nobody can read or modify the message during transfer
- Non-repudiation – to ensure that an entity cannot deny the authenticity of their signature on a document, or the sending of a message that they originated.
- Logging – to store legal proof of a message transfer. This could be the message itself, or a hash of the message. A message hash has four main properties: 1) easy to compute the hash value for any given message, 2) infeasible to generate a message from its hash, 3) infeasible to modify a message without changing the hash, 4) infeasible to find two different messages with the same hash.

In many solutions, the certification and non-repudiation concepts are missing. Logging is implemented in the central part (the service providers are not logging by default what data is requested from them). It is better if it is done on the publisher and subscriber environments, while the central component would only store a hash of the logs.

Evaluation score of current criteria: GovTalk - 2, WSO2 - 2, X-Road – 5, Highway - 2

3.4. Performance

The “performance” criterion is being considered in order to ensure minimal delay of message transfers. “Performance” determines the time it takes (i.e. the time-delay) to transfer a message, between organizations. Time-delays should be as short as possible. Performance is affected by the resource use (i.e. demand) of the message transfer software, by the resource capacity of the platform, and by the volume of message transfers at any specific moment.

In centralised solution message transfer is initiated by the sender by sending the message to the Portal. This implies that the centralised infrastructure is a performance bottleneck.

Evaluation score of current criteria: GovTalk - 3, WSO2 - 3, X-Road – 4, Highway 2

3.5. Availability

The “availability” criterion is being considered to ensure 24/7 availability of the infrastructure. Availability is dependent on many factors, including architecture (distributed or centralized), software distribution, operations resilience, and resilience against malware attacks. For a national secure message transfer infrastructure, 24/7 availability is mandatory.

Info Highway is vulnerable due to its centralized architecture. Maintenance or upgrades on the central software infrastructure will lead to lower availability.

Evaluation score of current criteria: GovTalk - 4, WSO2 - 4, X-Road – 5, Highway -3

3.6. Flexibility

The “flexibility” criterion is being considered to ensure optimal flexibility for connecting organizations. For a national, secure interoperability solution for agnostic message transfer, flexibility in message structures, message transformation and/or message processing is a non-issue. This is because the data sharing only requires transfer of bit/byte streams (i.e. agnostic message transfer). It is strongly advisable for the data sharing platform to limit itself to agnostic (without any knowledge of structure and content) message transfer only. Any message structure, transformation and/or processing is done at application levels, by the systems of the interoperating organisations.

Evaluation score of current criteria: GovTalk - 4, WSO2 - 5, X-Road – 3, Highway 3

3.7. Architecture

The “architecture” criterion is being considered to provide insight in the role and position between organizations’ systems. As architecture determines facilities such as security, performance and resilience, it is a one of the most important criteria for the data sharing platform.

In case of decentralised architecture (right, in figure below) messages are transferred directly between proxy software created ad-hoc at all the interoperating organizations. The proxies are asynchronously managed and monitored by central components. Because central components can also be replicated, the overall architecture of the data sharing platform proves resilient to error and to attacks.

In case of centralized architecture (left in figure below) messages are transferred by the interoperating organizations to/from the central infrastructure. The advantage is that message transformation and business process management are easy to manage centrally. However, this is a capability that is explicitly NOT wanted for an inter-organisation facility, because the connecting organizations will not defer their unique responsibilities to a central organization. However, for the eGovernment, the missing security features (certification and non-repudiation) are mandatory. A centralized architecture is also more vulnerable to internal (maintenance and updates) and external (hacking, DoS) disruptions.

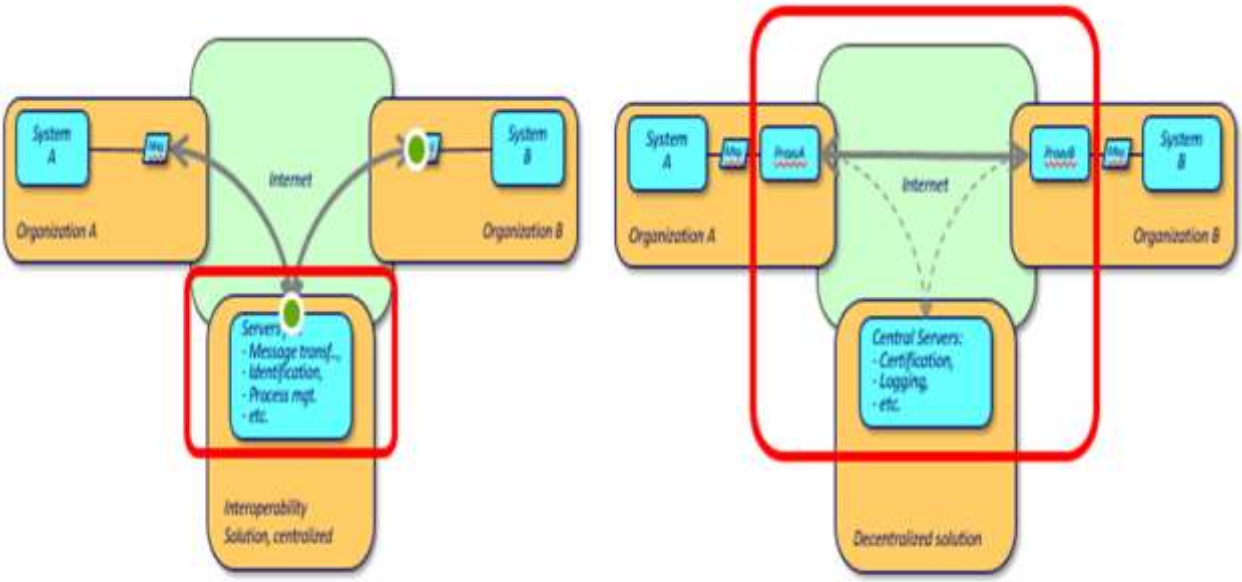

Figure 3 Centralised and decentralised architecture of data sharing platform

Evaluation score of current criteria: GovTalk - 3, WSO2 - 3, X-Road – 5, Highway - 2

3.8. Operations

The “operations” criterion is being considered to support easy operations, oversight, management and maintenance of the infrastructure. For the governance agency, as well as for the connecting organizations, smooth operations, monitoring, management, backup/restore, maintenance, upgrades, etc. are mandatory for a 24/7 facility as the eGovernment Information System.

Evaluation score of current criteria: GovTalk - 4, WSO2 - 4, X-Road – 4, Highway - 4

3.9. Scalability

The “scalability” criterion is being considered to support ever-growing numbers of message transactions. Scalability is the capability that, when the number of message transfers increases, low transfer times (response times) can be retained. Scalability can be achieved by replicating the components of the data sharing platform.

Highway is centralised system where all network traffic runs through central servers. Central servers may become a scalability bottleneck. Platform should be scalable without stopping data sharing functionalities.

Evaluation score of current criteria: GovTalk - 3, WSO2 - 3, X-Road – 5, Highway -2

3.10. Resilience

The “resilience” criterion is being considered to ensure 24/7 availability and continuity, under all circumstances. Resilience is the capability of an infrastructure to retain operations, irrespective of hardware, software or operator faults, or external threats. For a national infrastructure, resilience is one of the key attributes, since any failure to provide 24/7 availability may have large economic impacts. For example, the Estonian X-Road processes 2,000,000 transactions per day. It is unacceptable to have a downtime of the platform for even one minute. X-Road has had no breaks for over 5000 days and counting.

Centralised platforms are vulnerable, due to its centralized infrastructure, both to internal and to external threats. Message transfers stop when one of central servers fails, or if taken offline for maintenance or upgrades.

Evaluation score of current criteria: GovTalk - 2, WSO2 - 2, X-Road – 5, Higway - 2

3.11. Security

The “security” criterion is being considered to support identification, authentication, certification, encryption, nonrepudiation and logging of all message transfers.

The presence of end-to-end security properties such as non-repudiation is highly important.

Evaluation score of current criteria: GovTalk - 4, WSO2 - 4, X-Road – 5, Highway - 3

3.12. Support

The “support” criterion is being considered to ensure optimal support, internal and external, during the lifetime of the infrastructure.

Evaluation score of current criteria: GovTalk - 5, WSO2 - 4, X-Road – 4, Highway -3

3.13. Total Cost of Ownership

The “Total Cost of Ownership (TCO)” criterion is being considered to provide insight in all cost of hardware, operations, maintenance, upgrades and support, for a period of at least 3 years. Cost is always a factor to be considered. However, because the economic value of the interoperability infrastructure is orders of magnitude greater, in this case, cost is less important.

For obtaining Highway, WSO2, or X-Road there is no need to pay for a license. WSO2 and GovTalk (based on BizTalk) are enterprise oriented systems. Adaption for government needs additional resources. BizTalk is Microsoft product, it needs regular licence fee.

Evaluation score of current criteria: GovTalk - 2, WSO2 - 3, X-Road – 4, Highway - 4

3.14. Evaluation summary

Details of the weighted scores evaluation of four platforms are shown in the spider chart below.

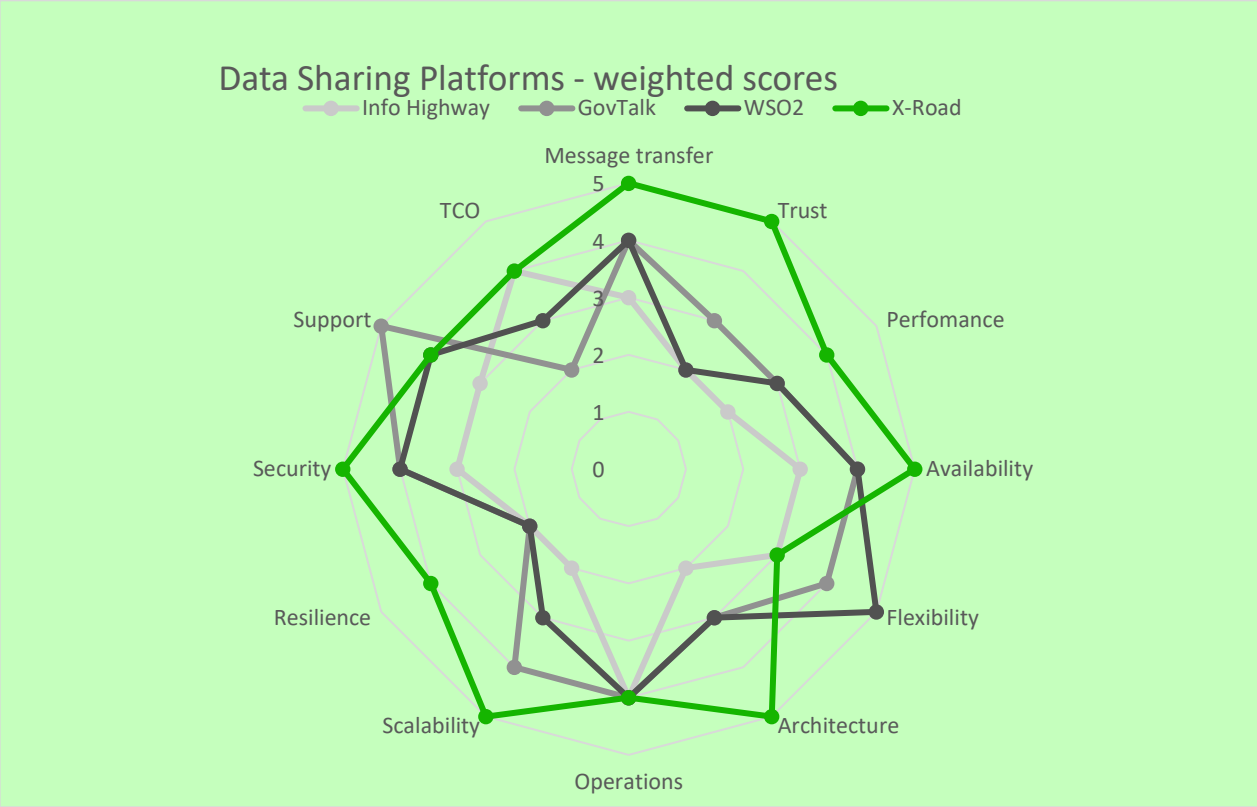

Figure 4. Data Sharing Platforms evaluation spider chart.

Summary:

- Highway - 33 points 55% from maximum;
- WSO2 – 41 points, 68%;
- GovTalk – 42 points, 70%;
- X-Road – 53 points, 88%.

NB: Not all criteria are important for eGovernment. For example, flexibility is important for enterprise systems, but not for Government where it is better to agree on a common format.

4. Technical Specification for secure data exchange

4.1. Overview

Technical specification depends what platform we use. X-Road is a system for enabling secure communication between organizations. This chapter describes technical architecture of the X-Road core. The goal is to give general overview of the X-Road system and the components that it contains. Detailed description of components and protocols can be found in separate documents. For information on the processes implemented by the X-Road components, refer to the use case documentation.

The following list contains main design goals and design decisions of the X-Road system.

- X-Road is **decentralized** – the data exchange happens directly between organizations. There are no intermediaries. If the two organizations have established secure connection, the continuous data exchange depends only on availability of the organizations and the network between them.
- **Ownership of data** – X-Road does not change ownership of data. The data owner (service provider) controls who can access particular services.
- **Availability** – the protocols are designed so that there is no single bottleneck in the system. Additionally, no component should become a single point of failure.
- All the messages processed by the X-Road are usable as **digital evidence**. The technical solution must comply with requirements for digital seals according to eIDAS. This implies support for secure signature creation devices (SSCDs).
- All the communication is implemented as **service calls** using the SOAP protocol. The services are described using the WSDL language.
- **Cross-border services** – it is possible for an organization to invoke services provided by an organization belonging to a different instance of X-Road.
- **Encapsulating the security protocol** – the security measures and the security protocol are encapsulated in standard components. The organizations are not required to implement security-related functionality for data exchange.
- **Standardization** – X-Road aims to standardize the communication protocol between organizations. This enables the organizations to connect to any number of service providers without implementing additional protocols. X-Road core does not perform protocol and data conversion. If necessary, these conversions can be performed by the organization's information system.
- **No predetermined roles** – once an organization has joined the X-Road infrastructure, it can act as both service client and service provider without having to perform any additional registration.
- **Two-level authentication** – X-Road core handles authentication and access control on the organization level. End-user authentication is performed by information system of the service client.

4.2. Components of X-Road

Figure 5 shows the main components and interfaces of the X-Road system. The components that are not part of the X-Road core are shown on grey background. The components and the interfaces are described in detail in the following sections.

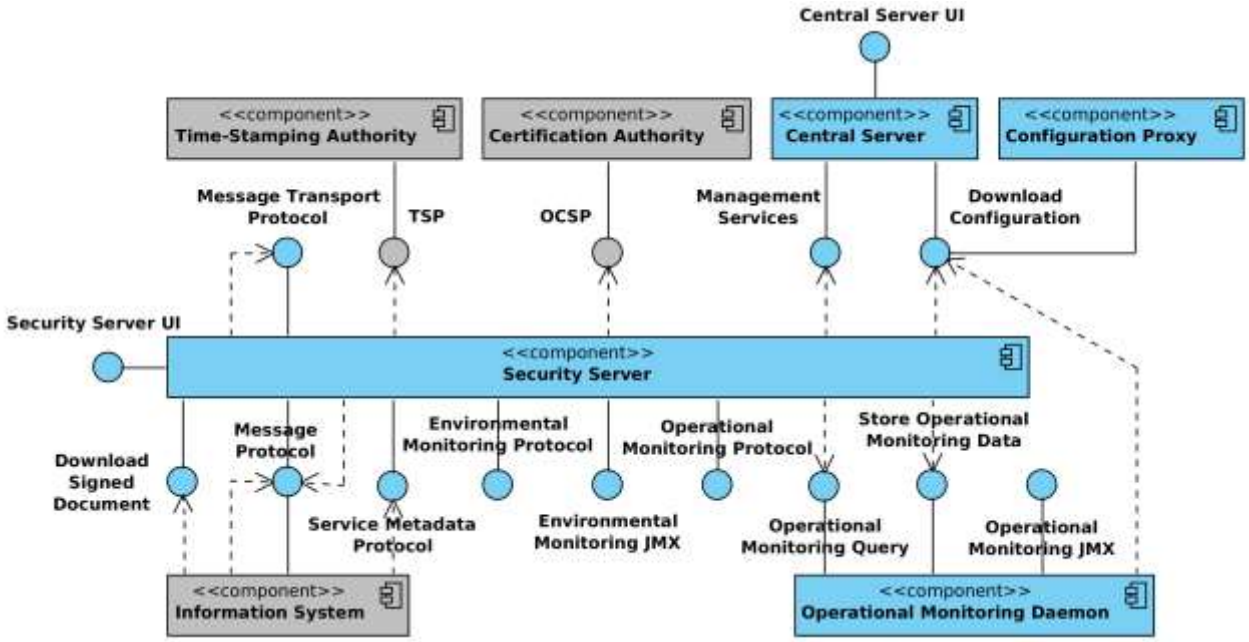

Figure 5. Logical structure of X-Road

4.2.1. Central Server

Central server manages the database of X-Road members and security servers. In addition, the central server contains the security policy of the X-Road instance. The security policy consists of the following items:

- list of trusted certification authorities,
- list of trusted time-stamping authorities,
- tunable parameters such as maximum allowed lifetime of an OCSP response.

Both the member database and the security policy are made available to the security servers via HTTP protocol. This distributed set of data forms the global configuration. In addition to configuration distribution, the central server provides interface for performing management tasks such as adding and removing security server clients. These tasks are invoked from the user interface of the security servers. The management services are implemented as standard X-Road services and offered via central security server.

4.2.2. Security Server

The security server (proxy gateway) mediates service calls and service responses between information systems. The security server encapsulates the security aspects of the X-Road infrastructure: managing keys for signing and authentication, sending messages over secure channel, creating the proof value for messages with digital signatures, time-stamping and logging. For the

service client and the service provider information system, the security server offers a SOAP-based protocol. This protocol is the same for both the client and the service provider, making the security server transparent to the applications.

A single security server can host several organizations (multi-tenancy). The organization managing the security server is the server owner, the hosted organizations are security server clients.

The security server manages two types of keys. The authentication keys are assigned to a security server and used for establishing cryptographically secure communication channels with the other security servers. The signing keys are assigned to the security server's clients and used for signing the exchanged messages. The keys can be stored either on hard disk (software token) or on an SSCD.

The security server downloads and caches up-to-date global configuration and certificate validity information. Caching allows the security server to operate even when the information sources are unavailable.

The security server contains an optional monitoring component that keeps track of environmental properties such as running processes, available disk space, installed packages etc. The monitoring component publishes this data via environmental monitoring service and monitoring JMX interfaces.

4.2.3. Information System

The information system (IS) uses and/or provides services via the X-Road.

For the service client IS, the security server acts as an entry point to all the X-Road services. The client IS is responsible for implementing a user authentication and access control mechanism that complies with the requirements of the particular X-Road instance. The identity of the end user is made available to the service provider by including it in the SOAP message. The client can discover the X-Road members and available services by using the X-Road metadata protocol.

The service provider information system implements a SOAP service and makes it available over the X-Road. For this purpose, the service must conform to the X-Road message protocol . The service must be accompanied by the service description implemented in the WSDL language.

4.2.4. Time-Stamping Authority

The time-stamping authority issues time stamps that certify the existence of data items at a certain point of time. X-Road uses batch time-stamping. This reduces the load of the time-stamping service. The load does not depend on the number of messages exchanged over the X-Road, instead it depends on the number of security servers in the system.

4.2.5. Certification Authority

The certification authority (CA) issues certificates to security servers (authentication certificates) and to X-Road member organizations (signing certificates). All the certificates are stored in the security servers. The CA must be able to process certificate signing requests conforming to PKCS10[3].

[3] Certification Request Syntax Standard. RSA Laboratories, PKCS #10

The CA must distribute certificate validity information via the OCSP protocol. The security servers cache the OCSP responses to reduce the load in the OCSP service and to increase availability. The load on the OCSP service depends on the number of certificates issued.

4.2.6. Configuration Proxy

The configuration proxy implements both the client part and the server part of the configuration distribution protocol. The configuration proxy downloads the configuration, stores it, and makes it available for download. Thus, the configuration proxy can be used to increase system availability by creating an additional configuration source and reduce load on the central server.

4.2.7. Operational Monitoring Daemon

The main functionality of the operational monitoring daemon is to collect and store operational data of the X-Road security server and make it available for external monitoring systems via corresponding interfaces.

4.3. Deployment View

Figure 6 shows deployment view of a basic X-Road instance. In practice, all the components can use redundancy to improve availability and throughput. The deployment options for various components are described in the detailed architecture documents.

The diagram also shows what components are installed and hosted by any given organization. The governing authority installs and maintains central server and central security server. The configuration proxy is an optional component that is typically used for distributing configuration to federated X-Road instances. The service client and service provider organizations host their information system and security server that connects the information system to the X-Road.

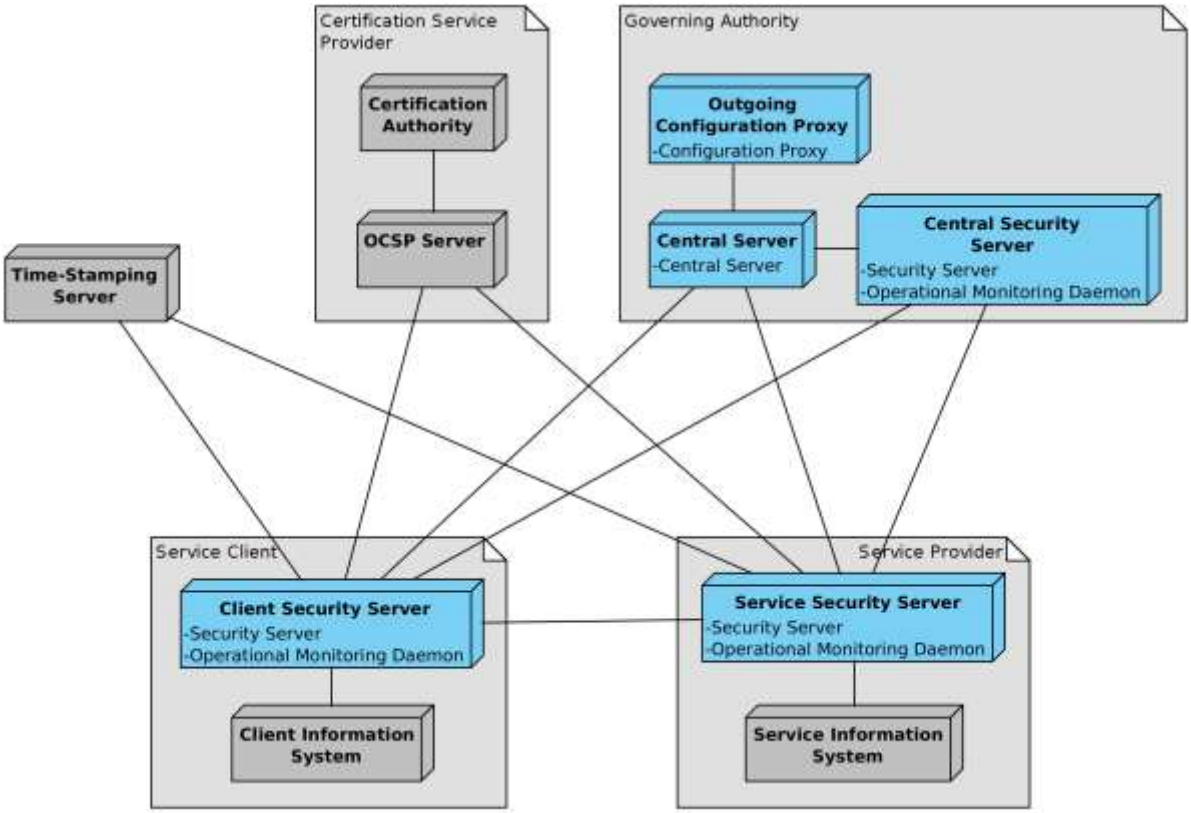

Figure 6. Deployment view of X-Road

The implementation of X-Road assumes clear fixing responsibilities between stakeholders. Recommended distribution of responsibilities among members of X-Road:

Coordinating body. Coordination, financing and supervision function

Implementing body. Implementing and maintenance X-Road. Responsible for X-Road governance (central servers, monitoring server) and trust services (certification of persons and organisations).

Service providers (owners of registries) will operate service security server, build adapters for services, open services for consumers.

Service clients are function as front end systems. Service clients are agencies, portals owners and local government bodies. They will operate client security servers, build adapter in client information systems or use standard solution MISP (Mini Information System Portal). Adding new services to the portal will be simple. Portal will have functionalities for automatic generating service interfaces (for example from WSDL and XForms descriptions) and service aggregation tools (results of the one service are used as a parameter for other service). Logical view of service client architecture presented in figure below.

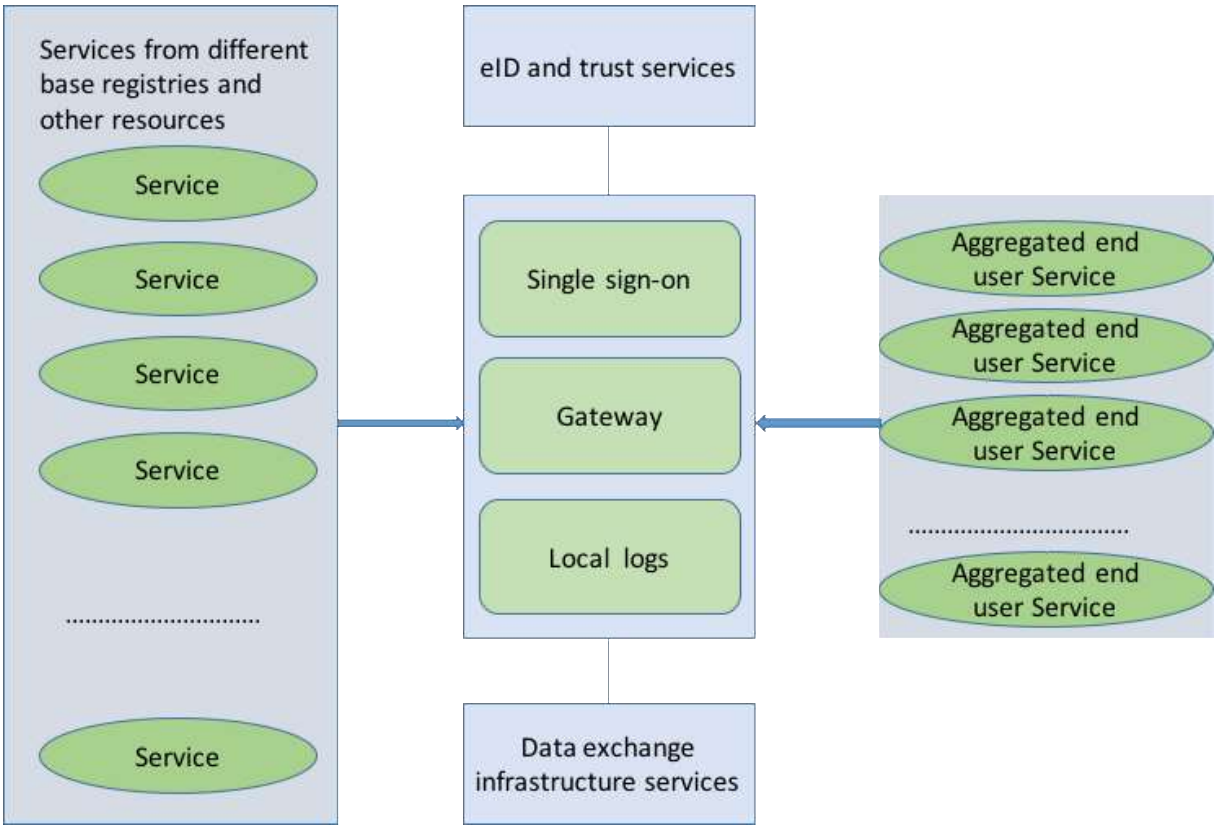

Figure 7. Aggregation and presentation services for end users through front-end systems

4.4. Set of Documentation on Technical Specifications and Standards

X-Road has thoroughly described, there exist learning material and source code is available as open source software. The full set of architecture is listed below. Items of documentation contains links to the concrete documentation in X-Road github: https://github.com/ria-ee/X-Road

4.4.1. Architecture

- X-Road Architecture
- Security Server Architecture
- Configuration Proxy Architecture
- Central Server Architecture
- Audit Log Events

4.4.2. Protocols

- Message Protocol
- Message Transport Protocol
- Protocol for Management Services
- Service Metadata Protocol
- Protocol for Downloading Configuration

4.4.3. Manuals

- Security Server User Guide
- Central Server User Guide
- Signer Console Users Guide
- Security Server Installation Guide
- Central Server Installation Guide
- HA Installation Guide
- Signed Document Download and Verification Manual
- Configuration Proxy Manual
- System Parameters
- External Load Balancer Installation Guide

4.4.4. Use Cases

- Security Server Management
- Configuration Proxy
- Central Server Management
- Federation
- Member Management
- Global Configuration Distribution
- Trust Service Management
- Member Communication
- Service Management

4.4.5. Data Models

- Security Server Configuration
- Central Server Configuration
- Message Log

4.4.6. Monitoring

- Environmental Monitoring Architecture
- Environmental Monitoring Messages

4.4.7. Additional components of X-Road

- X-Road Portal MISP2
- X-Road WSDL validator
- X-Road Personal Data Monitor
- X-Road Generator (X-tee .NET)
- J-road
- REST-Gateway
- XRd4J

- SAP PI X-Road Adapter
- XRDv4WSDLConverter
- X-Road Adapter Example
- X-Road Test Service
- X-Road Test Client
- Qure Data Management Platform

4.4.8. Learning material

You can find learning material from https://moodle.ria.ee/. Most important trainings are available in English:

- Learning material for X-Road security server administrator
- Training materials for developers of X-Road interfaces

5. Protocols and Interfaces

The use of X-Road does not need changes in existing systems. In this chapter, we summarise the protocols and interfaces of X-Road. You can find detailed description from documentation (see 5.4).

5.1. X-Road Message Protocol

X-Road Message Protocol is used by service client and service provider information systems for communicating with the X-Road security server. The protocol is a synchronous RPC style protocol that is initiated by the client IS or by the service provider's security server.

The X-Road Message Protocol is based on SOAP over HTTP(S) and adds additional header fields for identifying the service client and the invoked service.

This protocol (together with the Message Transport Protocol) forms the core of the X-Road data exchange. If the involved components are not available, then the data exchange is not possible. X-Road architecture makes possible to improve the availability of the involved components by using redundancy.

5.2. Protocol for Downloading Configuration

Configuration clients download the generated global configuration files from the central server. The configuration download protocol is a synchronous protocol that is offered by the central server. It is used by configuration clients such as security servers and configuration proxies.

The protocol is based on HTTP and MIME multipart messaging. The configuration is signed by the central server to protect it against modification. Usually the configuration consists of several parts. The protocol allows configuration clients to check whether the configuration has changed and only download the modified parts.

X-Road security servers (and operational monitoring daemons) maintain a local copy of the global configuration, which they periodically update from their respective configuration source. This cached global configuration has a validity period, which, in general, is longer than the period at which configuration clients are configured to update their local copy. Security servers continue to be fully operational while the cached global configuration remains valid. However, an out-of-date copy of the global configuration severely restricts the management capabilities of security server administrators and forbids security servers from processing incoming requests. As such, a short downtime of the interface is permissible within the limits of the configured configuration validity period.

5.3. Message Transport Protocol

The X-Road Message Transport Protocol is used by security server to exchange service requests and service responses. The protocol is a synchronous RPC style protocol that is initiated by the security server of the service client.

The protocol is based on HTTPS and uses mutual certificate-based TLS authentication. The SOAP messages received from the client and the service provider IS are wrapped in MIME multipart message together with additional security-related data, such as signatures and OCSP responses.

This protocol (together with X-Road message protocol) forms the core of the X-Road data exchange. If the involved components are not available, then the data exchange is impossible. X-Road architecture makes possible to improve the availability of the involved components by using redundancy.

5.4. Service Metadata Protocol

The X-Road Service Metadata Protocol can be used by the service client information systems to gather information about the X-Road instance. In particular, the protocol can be used to find X-Road members, services offered by these members and the WSDL service descriptions.

The protocol is a synchronous RPC style protocol that is initiated by the service client IS. Some of the information services are implemented as HTTP(S) GET requests to simplify client IS implementation. The other information services are called as standard X-Road services

The Service Metadata Protocol is used for client IS configuration and therefore the availability, throughput and latency of its implementing components are not critical to the functioning of the X-Road.

5.5. Download Signed Document

The service for downloading signed documents can be used by the information systems to download signed containers from the security server's message log. In addition, the service provides a convenience method for downloading global configuration that can be used to verify the signed containers.

The protocol is a synchronous RPC-style protocol that is initiated by the IS. The service is implemented as HTTP(S) GET requests.

The Download Signed Document protocol is used by IS for downloading data stored in the security server and therefore the availability, throughput and latency of its implementing components are not critical to the functioning of the X-Road.

5.6. Management Services Protocol

The management services are called by security servers to perform management tasks such as registering a security server client or deleting an authentication certificate. The management service protocol is a synchronous RPC-style protocol that is offered by the central server. The service is called by security servers.

The management services are implemented as standard X-Road services that are offered by the organization managing the X-Road instance. The exception is the authentication certificate registration service that, for technical reasons, is implemented directly by the central server.

In general, the management services are not critical to operation of X-Road and therefore their availability is not paramount. If the management services are unavailable, the security servers cannot manage their clients and authentication certificates. Some actions (such as removing clients and certificates) can be performed manually by central server administrator, without using the management services. The management service operations are not time-critical (the security server

user explicitly chooses to send the management request and the user interface does not imply that this operation is instantaneous).

5.7. OCSP Protocol

The OCSP protocol is used by the security servers to query the validity information about the signing and authentication certificates. OCSP protocol is synchronous protocol that is offered by the OCSP responder belonging to a certification authority.

In X-Road, each security server is responsible for downloading and caching the validity information about its certificates. The OCSP responses are sent to the other security servers as part of the message transport protocol . This ensures that the security servers do not need to discover the OCSP service used by the other party. Additionally, this arrangement supports the situation where access to the OCSP service is either restricted to certificate owners or is subject to charges.

The security servers never include nonce field in the OCSP request. This allows the OCSP service to employ various optimization strategies, such as pre-creating the OCSP responses.

Because OCSP responses are used in the process of certificate validation, failure of the OCSP service effectively disables X-Road message exchange. When the cached OCSP responses cannot be refreshed, the security servers are unable to communicate. Thus, the lifetime of the OCSP responses determines the maximum amount of time that the OCSP service can be unavailable. The lifetime is defined by the owner of the central server and can vary between different instances of X-Road.

5.8.Time-Stamping Protocol

The Time-stamping protocol is used by security servers to ensure long-term proof value of the exchanged messages. The security servers log all the messages and their signatures. These logs are periodically time-stamped to create long-term proof.

Time-stamping protocol is a synchronous protocol that is provided by the time-stamp authority. However, the security servers use the time-stamping protocol in an asynchronous manner. Security servers log all the messages that are exchanged with other security servers. These messages are time-stamped asynchronously using batch time-stamping. This is done to decouple availability of the message exchange from availability of the time-stamping authority, to decrease the latency of message exchange, and to reduce load on the time-stamping authority.

Because time-stamping is used in an asynchronous manner, temporary unavailability of the time-stamping service does not directly affect the X-Road message exchange. However, if the security servers fail to time-stamp the accumulated messages for certain time period then it may become difficult to prove the exact time of the message exchanges. To minimize this risk the security servers will stop forwarding messages if the time-stamping has been failing for some time. The maximum allowed time period between logging of a message and acquiring a time stamp for that message is defined by the owner of the central server and can very between different instances of X-Road.

5.9. Security Server User Interface

The security server user interface is used by the security server administrator to configure and manage the security server.

5.10. Central Server User Interface

The central server user interface is used by the central server administrator to configure and manage the central server.

5.11. Store Operational Monitoring Data

This protocol is used by the X-Road security server to store its cached operational monitoring data into the database of the operational monitoring daemon. The protocol is a synchronous RPC-style protocol based on JSON over HTTP(S).

5.12. Operational Monitoring Query

The operational monitoring query interface is used by the X-Road security server to retrieve operational monitoring data from the operational monitoring daemon. The asynchronous RPC-style X-Road operational monitoring protocol is used.

5.13. Operational Monitoring Protocol

This interface is used by external monitoring systems to gather operational information of the security server. The protocol is synchronous RPC style protocol that is initiated by the external monitoring system.

5.14. Operational Monitoring JMX

This interface is used by a local monitoring system (e.g. Zabbix) to gather local operational health data of the security server via JMXMP.

5.15. Environmental Monitoring Protocol

The environmental monitoring interface responds to queries for monitoring environmental data from security server's server/proxy interface. The environmental monitoring data is collected by environmental monitoring service.

5.16. Environmental Monitoring JMX

The environmental monitoring JMX service publishes environmental monitoring data via JMX interface. The environmental monitoring data is collected by environmental monitoring service.

9. Interoperability agreements and standards

Provision of data sharing services requires cooperation between different organizations. Such cooperation takes place at the different interoperability levels. For each level, the organisations involved should formalise their cooperation in interoperability agreements. These agreements should be drafted with sufficient level of detail so that they achieve the intended result while leaving each organisation maximal internal autonomy.

At the **legal level**, interoperability agreements are expressed in concrete and binding terms, via legislation.

At the **organisational level**, interoperability agreements can take the form of SLA's that specify the obligations of each party participating in data sharing. Interoperability agreements at the organisational level will define expected levels of services, support/escalation procedures, contact details, etc. referring, when necessary, to underlying agreements at the semantic and technical levels.

At the **semantic level**, interoperability agreements take the form of, inter alia, reference taxonomies, schemes, code lists, data dictionaries or sector-based libraries.

At the **technical level**, interoperability agreements will include items such as communication protocols, messaging specifications, data formats, security specifications or dynamic registration and service discovery specifications.
Following diagram illustrates the need of interoperability standards[4]:

[4] Based on: Michiel Malotaux. e-Government Interoperability Solution. The Vision Labs. 9 May 2016.

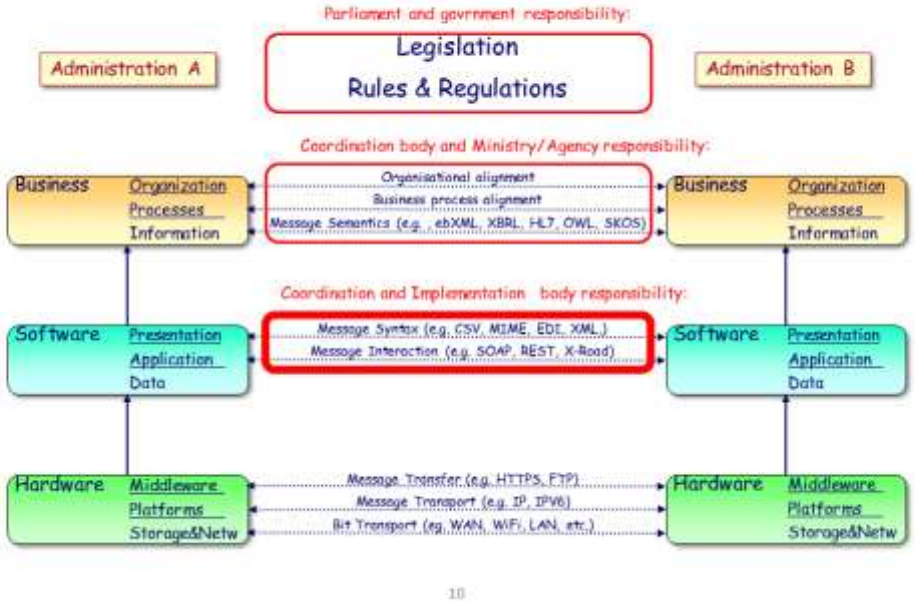

Figure 8. Interoperability agreements and standards on the different layers

Standards are defined, maintained and evolved by standards committees – network and message transfer standards are global, domain (e.g. government, healthcare, transport, etc.) may be global, regional or national. Standards are adopted and supported on the different levels of the e-Government infrastructure.

Imposing detailed technical standards can damage competition and innovation, isolate public sector from the broader technological trends and, finally, it distracts resources from more important interoperability issues[5]. Public sector agrees on the minimum set of open standards, compliance with which is compulsory. The choice and assessment of standards must be public and balanced. With regard to in-house communication, institutions are allowed, although it is not recommended, to use other standards.

Below is the list of recommended open standards and agreements regularly used:

- CSV (Comma Separated Values)[6] – platform-independent format for tabular data;
- HTML (HyperText Markup Language)[7] – hypertext markup language for creating web documents;
- CSS (Cascading Style Sheets)[8] - language used for describing the presentation of a document written in a markup language;

[5] See more: e-Government Interoperability. A comparative analysis of 30 countries. http://www.cstransform.com/resources/white_papers/InteropAnalysisV2.0.pdf

[6] http://tools.ietf.org/html/rfc4180

[7] http://www.w3.org/wiki/HTML

[8] www.w3.org/TR/REC-CSS2/

- EIDAS EU Regulation No 910/2014 – Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[9]
- JPEG (Joint Photographic Experts Group [.jpg])[10] – compression method and file format of digital images;
- OGC (Open GIS)[11] formats for exchange of geospatial data and standards of digital geographic information by the ISO/TC 211 committee;
- GZIP[12] – package format
- MPEG (Moving Picture Experts Group [.mpeg])[13] – video format
- ODF (Open Document Format [.odf])[14] – open document format for office applications ; ODF sub-formats are .odb (database), .odf (formula), .odg (drawing), .odp (presentation), .ods (spreadsheets) ja .odt (texts)
- PDF (Portable Document Format [.pdf])[15] – platform independent document format
- PDF/A (Portable Document Format/Archive) format for archiving .pdf files
- RFC3161. Time-Stamp Protocol[16]
- RSA cryptosystem[17]
- SOAP (Simple Object Access protocol)[18] is a protocol specification for exchanging structured information in the implementation of web services in computer networks.
- PNG (Portable Network Graphics [.png])[19] – raster graphics format
- PKI (Public Key Infrastructure)
- SVG (Scalable Vector Graphic [.svg])[20] – vector graphics format
- TIFF (Tagged Image File Format [.tif])[21] – raster graphics format
- TXT (Plain Text, Text File [.txt]) – plain unprocessed text format
- TSL (Trust Service list)[22]
- XAdES (XML Advanced Electronic Signatures) [23]

---

[9] http://eur-lex.europa.eu/eli/reg/2014/910/oj
[10] ISO 10918 (.jpg), http://www.jpeg.org/index.html
[11] http://www.opengeospatial.org/standards
[12] RFC 1952
[13] MPEG4/ISO/IEC 14496
[14] ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument)
[15] ISO 32000-1:2008
[16] https://www.ietf.org/rfc/rfc3161.txt
[17] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[18] http://www.w3.org/TR/soap/
[19] http://www.w3.org/TR/REC-png
[20] http://www.w3.org/TR/SVG/
[21] http://tools.ietf.org/html/rfc2306
[22] http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf
[23] https://www.w3.org/TR/XAdES/

- XML (Extensible Hypertext Markup Language [.xml])[24] – hypertext markup language
- XSL (Extensible StyleSheet Language)[25]
- X.509. Format of public key certificates[26]
- WSAG (Web Content Accessibility Guidelines)[27]
- WSDL (Web Services Description Language)[28] is an XML-based interface definition language that is used for describing the functionality offered by a web service

The level of openness of a formalised specification is an important element in determining the possibility of sharing and reusing software components implementing that specification. If the openness principle is applied in full:

- all stakeholders have the same opportunity to contribute to the development of the specification and a public review is part of the decision-making process;
- the specification is available for everybody to study;
- intellectual property rights related to the specification are licensed on FRAND (fair, reasonable, and non-discriminatory) terms or preferably on a royalty-free basis in a way that allows implementation in both proprietary and open source software.

However, public administrations may decide to use less open specifications if open specifications/standards do not exist or do not meet functional interoperability needs. In all cases, specifications should be mature and sufficiently supported by the market, except if used in the context of creating innovative solutions

[24] http://www.w3.org/XML/
[25] www.w3.org/TR/xsl/
[26] http://www.itu.int/rec/T-REC-X.509/en
[27] http://www.w3.org/TR/WCAG20/
[28] http://www.w3.org/TR/wsdl