

TESLA INSTITUTE

# X-Road® Fundamentals



Peter Witt



# Contents

Contents.....	2
Introduction.....	8
Welcome.....	8
Getting started.....	8
Technology overview.....	9
Organisational model.....	13
Architecture.....	15
Community.....	20
Terms and abbreviations.....	21
X-Road and X-Road instance.....	21
Participants of X-Road.....	22
Trust services.....	23
Roles of X-Road client.....	25
X-Road interfacing steps.....	26
Elements of X-Road software.....	27
X-Road protocols.....	30
Logging and security.....	30
Identifiers and codes.....	31
Global configuration concepts.....	33
Technical terms.....	36
Implementation models.....	38
Introduction.....	38
National data exchange layer.....	38
Data exchange solution for regions.....	40
Data exchange within a business domain or sector.....	41
A platform for data exchange within an organisation.....	42

---

Architecture.....	44
Introduction.....	44
System components.....	47
Protocols and interfaces.....	52
Deployment view.....	61
Security Architecture.....	62
Introduction.....	62
Environment Assumptions.....	64
Confidentiality.....	64
Integrity.....	65
Availability.....	65
Authentication and access control.....	67
Authentication.....	67
Access Control.....	68
Input validation and logging.....	69
Input Validation.....	69
Logging.....	70
Time-stamping and updatability.....	72
Time-Stamping.....	72
Updatability.....	72
Trust federation.....	73
Standardised protocols.....	74
Central Server and Security Server.....	76
Central Server.....	76
Security Server.....	77
Certificates and key management.....	78
Monitoring.....	79
Monitoring.....	79
Privacy and regulatory compliance.....	81

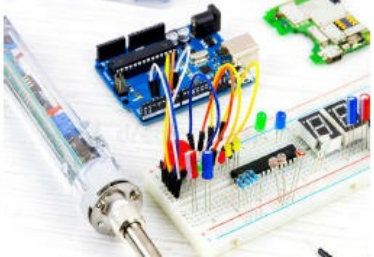
Privacy.....81  
Regulatory Compliance.....82



Course: EE02000  
**AUTOMATION and ELECTRONICS  
TECHNICIAN**



Course: EEE0120  
**Electronics with  
Microcontrollers Programming**



Course: EEE0100  
**ELECTRONICS  
TECHNICIAN**



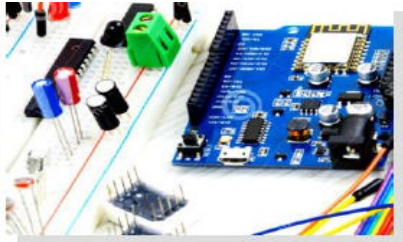
Course: EE01000  
**ELECTRICIAN  
TECHNICIAN**



Course: CT01000  
**COMPUTER TECHNOLOGY  
TECHNICIAN**



Course: EEE0130  
**Microcontrllers Programming**



Course: EE02100  
**Introduction to Programmable Logic Controllers (PLC)**



**TESLA INSTITUTE**  
Electrical Engineering School

## Like TESLA INSTITUTE Page



## Subscribe our Youtube channel



## Learn more with Young English Engineer



# Introduction

## Welcome

Welcome to the X-Road® Fundamentals! This book is the starting point of your X-Road learning path.

The book consists of five chapters:

- Introduction
- Terms and abbreviations
- Implementation models
- Architecture
- Security Architecture

After all the chapters have been completed, there's an exam to test your X-Road knowledge.

## Getting started

### What is X-Road and what it does?

X-Road® is open-source software and ecosystem solution that provides unified and secure data exchange between organisations.





The basic idea of X-Road is that members of an ecosystem exchange data through access points (Security Servers) that implement the same technical specifications.

X-Road is a digital public good verified by the [Digital Public Goods Alliance](#), and it's released under the [MIT open source license](#) and is available free of charge.

## Technology overview

X-Road is a centrally managed distributed data exchange layer between information systems that provides a standardized and secure way to produce and consume services.

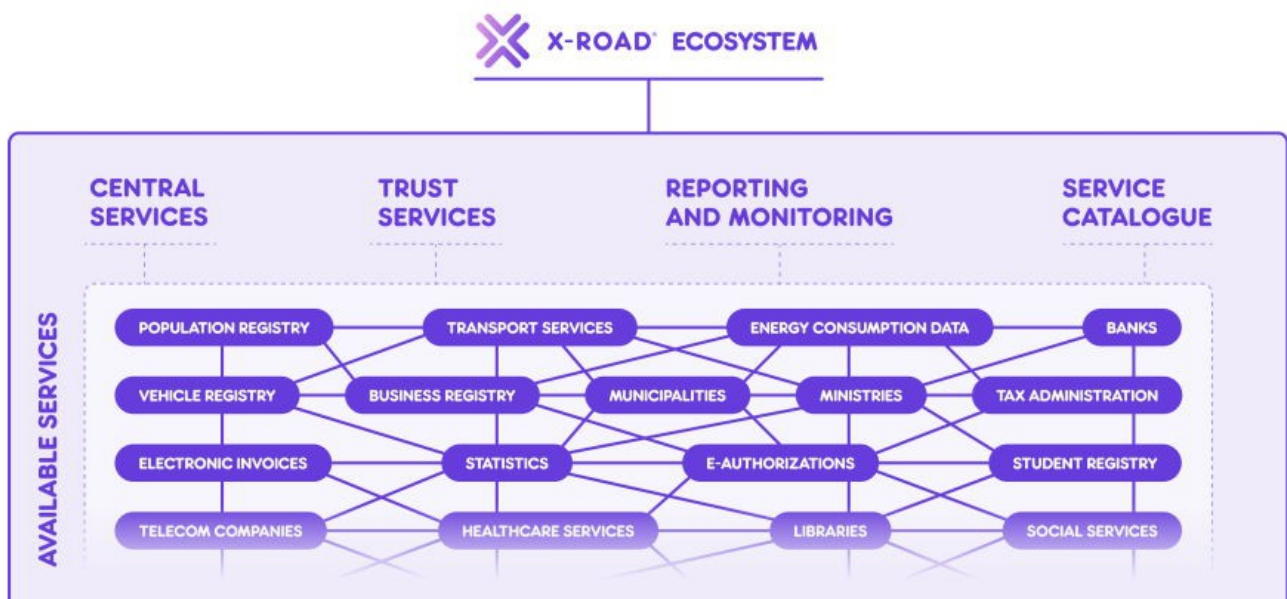
X-Road implements a set of standard features to support and facilitate data exchange and ensures confidentiality, integrity, and interoperability between data exchange parties:

- address management
- message routing
- access rights management
- organization-level authentication
- machine-level authentication
- transport-level encryption
- time-stamping
- digital signature of messages

- logging
- error handling.

## X-Road Ecosystem

An X-Road ecosystem is a community of organizations using the same instance of the X-Road software for producing and consuming services. The owner of the ecosystem, the X-Road Operator, controls who are allowed to join the community, and the owner defines regulations and practices that the ecosystem must follow.



The ecosystem may be nationwide, or it may be limited to organizations meeting specific criteria, e.g., clients of a commercial service provider. Technically, the X-Road software does not set any limitations to the size of the ecosystem or the member organizations.

## Trusted Network

Even if X-Road software is open-source, joining an X-Road ecosystem requires going through an onboarding process. During the process, the identity of each organization and technical access point is verified using certificates that are issued by a trusted Certification Authority (CA). The identities are maintained centrally, but all the data is exchanged directly between a service consumer and a service provider.

Message routing is based on organization and service level identifiers that are mapped to physical network locations of the services by X-Road. All the evidence regarding the data exchange is stored locally by the data exchange parties, and no third parties have access to the data. Time-stamping and digital signature together guarantee non-repudiation of the data sent via X-Road. The logs provided by X-Road can be used in a court proceeding as evidence.

## Authorization Framework

X-Road implements an authorization framework that is used to manage access rights to services. Access rights management is based on the organization and service level identifiers.

The key idea of X-Road is that each service provider owns its data and is responsible for managing access rights of its services. In other words, publishing service to X-Road does not mean that the service is automatically accessible to all X-Road member organizations. Usually, access rights are granted on the information system level – a service provider grants a specific information system access to a service.

## Monitoring and Reporting

X-Road provides monitoring and reporting capabilities that can be used to collect operational reporting data and technical monitoring information from the ecosystem. The information can be used to measure the usage of individual services, understand dependencies and relationships between different information systems and services, monitor service health, monitor used X-Road software versions, etc. Each X-Road member organization can access its own data, whereas the X-Road operator can access all the members' data.

## Cross-border Data Exchange

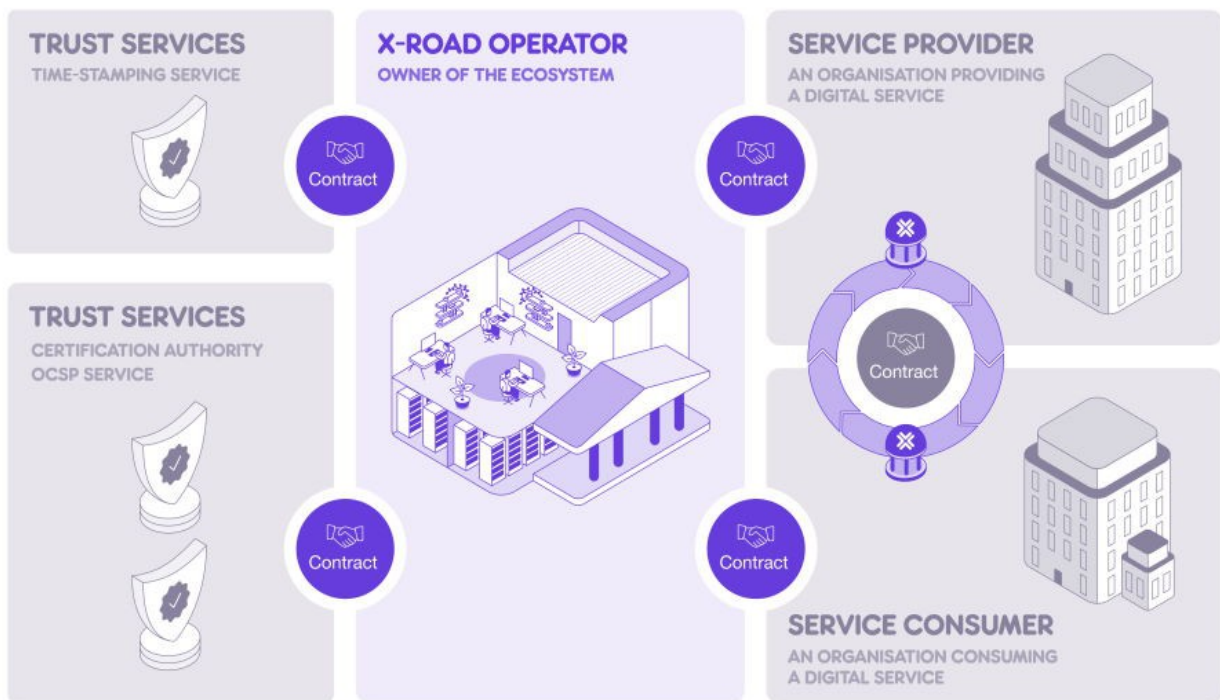
X-Road provides built-in support for cross-border data exchange through federation, which means joining together two X-Road ecosystems. Members of the federated ecosystems can publish and consume services with each other as if they were members of the same ecosystem.

It is possible to create federation connections with multiple ecosystems, but transitive federation relationships are not supported. An ecosystem does not have a federation relationship with another ecosystem that it's not directly federated with.

# Organisational model

X-Road ecosystem consists of an **X-Road Operator**, **Member** organizations, and **Trust Service Provider(s)**.

## X-ROAD ECOSYSTEM



## X-Road Operator

As the owner of the X-Road ecosystem, the Operator is responsible for

all the aspects of the operations. The responsibilities include defining regulations and practices, accepting new members, providing support for Members, and operating the central components of the X-Road software.

## **X-Road Members**

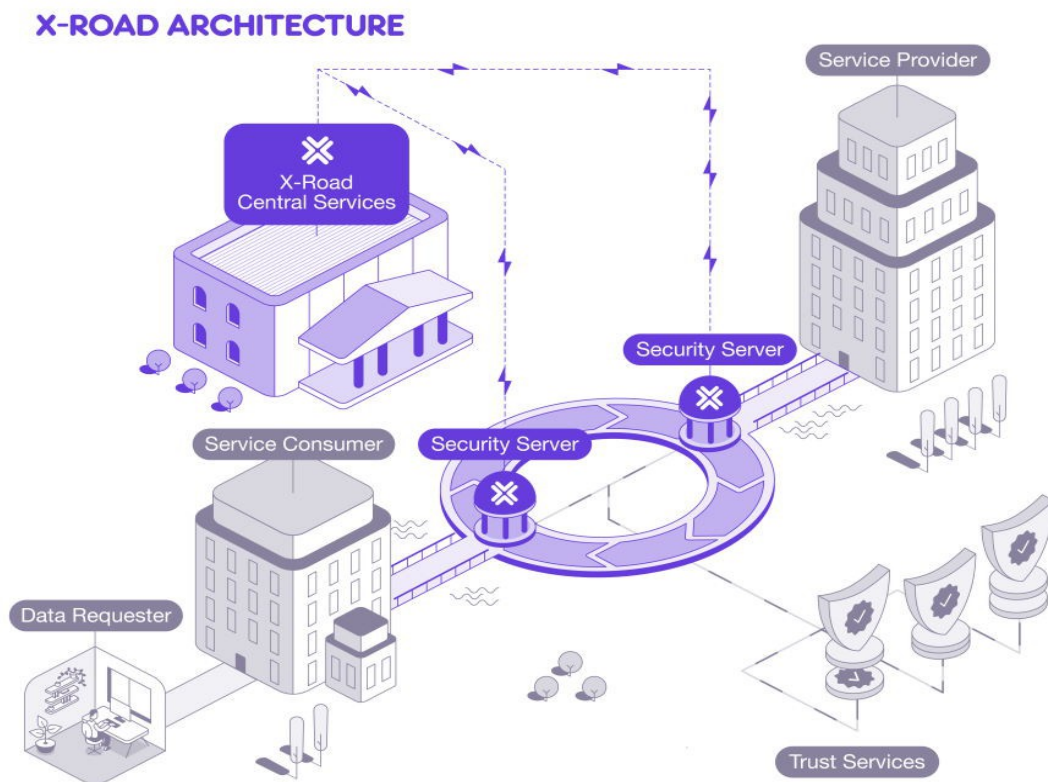
X-Road Members are organizations that have joined the ecosystem and produce and/or consume services with other Members. A Member organization can be a service provider, a service consumer, or both. Organizations can become Members of an ecosystem by completing the onboarding process defined by the Operator. Also, members need to have access to the technical component that is required for exchanging messages via X-Road, the Security Server.

## **Trust Service Provider(s)**

A functioning X-Road ecosystem requires two types of trust services: 1) time-stamping authority (TSA) and 2) certification authority (CA). Trust Service Providers are organizations providing these services. Trust Service Providers may be commercial third parties, or the services can be provided and maintained by the X-Road Operator too.

# Architecture

Technically X-Road ecosystem consists of Central Services, Security Servers, Information Systems, TSA(s), and CA(s).



## Central Services

Central services consist of Central Server and Configuration Proxy. Central Server contains the registry of X-Road members and their Security Servers. Besides, the Central Server contains the security

policy of the X-Road instance that includes a list of trusted certification authorities, a list of trusted time-stamping authorities, and configuration parameters. Both the member registry and the security policy are made available to the Security Servers via HTTP protocol. This distributed set of data forms the global configuration that Security Servers use for mediating the messages sent via X-Road. The X-Road Operator is responsible for operating the Central Server.

Configuration Proxy is an optional component that can be used as a proxy for publishing the global configuration to Security Servers for download. The Configuration Proxy first downloads the global configuration from the Central Server and then further distributes it securely. The Configuration Proxy can be used to increase system availability by creating an additional configuration source and reduce the load on the Central Server. The X-Road Operator is responsible for operating the Configuration Proxy.

## Security Server

Security Server is the entry point to X-Road, and it is required for both producing and consuming services via X-Road. The Security Server 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 a secure channel, creating the proof value for messages with digital signatures, time-stamping and logging. For a service consumer and a service provider Information System, the Security Server offers a REST-based and a SOAP-based message protocol. The 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, and 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 other Security Servers. The signing keys are assigned to the Security Server's clients and used for signing the exchanged messages. A trusted certification authority issues certificates for the keys. Certificates issued by other certification authorities are considered invalid.

To be able to mediate messages, the Security Server must have a valid copy of the global configuration available all the time. The Security Server downloads the global configuration from the Central Server regularly and uses a local copy while processing messages. The Security Server remains operational as long as it has a valid copy of the global configuration available locally. Similarly, certificate validity information is downloaded from the Certificate Authority and cached locally. Caching allows the Security Server to operate even when the configuration data sources are unavailable.

The Security Server has an internal client-side load balancer, and it also supports external load balancing. The client-side load balancer is a built-in feature, and it provides high availability. Instead, external load balancing provides both high availability and scalability from a performance point of view.

## Information System

The Information System produces and/or consumes services via X-Road and is owned by an X-Road member. X-Road supports consuming and producing both REST and SOAP services. However, X-Road does not provide automatic conversions between different types of messages and services.

For a service consumer Information System, the Security Server acts as an entry point to all the X-Road services. The consumer can discover registered X-Road members and their available services by using the X-Road metadata protocol.

A service provider Information System implements a REST and/or SOAP service and makes it available over the X-Road. Existing REST services do not require any changes – they can be published as-is. Instead, SOAP services must implement the X-Road message protocol for SOAP. Service descriptions of REST services are defined using OpenAPI3 specification, and service descriptions of SOAP services are defined using WSDL. Service consumers can download service descriptions using the X-Road metadata protocol.

## Time-Stamping Authority (TSA)

All the messages sent via X-Road are time-stamped and logged by the Security Server. The purpose of the time-stamping is to certify the existence of data items at a certain point in time. The TSA provides a time-stamping service that the Security Server uses for time-stamping all the incoming/outgoing requests/responses. Only trusted TSAs that

are defined in the Central Server can be used.

The time-stamping authority must implement the time-stamping protocol supported by X-Road. X-Road uses batch time-stamping, which 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.

## **Certification Authority (CA)**

The certification authority (CA) issues certificates to Security Servers (authentication certificates) and X-Road member organizations (signing certificates). Authentication certificates are used for securing the connection between two Security Servers. Signing certificates are used for digitally signing the messages sent by X-Road members. Only certificates issued by trusted certification authorities that are defined in the Central Server can be used.

The Security Server checks the validity of the signing and authentication certificates via the Online Certificate Status Protocol (OCSP). Each Security Server is responsible for querying the validity information of its certificates and then sharing the information with other Security Servers as a part of the message exchange process. Only Security Servers with valid signing and authentication certificates can exchange messages with other Security Servers.

# Community

The global X-Road Community is for anyone interested in X-Road. It's about learning from others and sharing the skills and experiences of how to create better digital services both technically and business-wise.

At its best, the community can be about reusing solutions other organizations have already created. It makes more sense for developers to post their questions to a community, because another organization may already have a solution or have experienced a similar issue.

[Events](#) for the community members are organized annually. There are also plenty of [resources](#) available for supporting the developers. [Join](#) the discussions on Slack!

# Terms and abbreviations

This section makes you familiar with terms and abbreviations commonly used in X-Road.

## X-Road and X-Road instance

**External X-Road instance** – an instance that has been federated with the local instance. For example, the FI-instance is defined as an external instance in the EE's local point of view.

**Local X-Road instance** – a group of members that are registered in a particular instance.

**United/federated X-Road** – a legal, organizational and technical environment, enabling universal internet-based secure data exchange between the members of united/federated X-Road instances

**X-Road instance** – a legal, organizational and technical environment, enabling universal internet-based secure data exchange between the members of X-Road and limited to the participants administered by one governing authority.

## Participants of X-Road

**Approved trust service provider** – participant of X-Road, who meets the requirements established by X-Road governing authority and has passed the process of recognition of X-Road trust service provider.

**End user of dataservice** – information system, part of information system or physical person, who uses data service through the information system of X-Road member.

**Local member** – a member entitled to exchange data/messages on the united X-Road and managed by governing authority of the local X-Road instance.

**United / Federated member** – a member entitled to exchange data/messages on their behalf on the united X-Road, but managed by governing authority of the external X-Road instance.

**X-Road Center** – participant of X-Road administering components of the X-Road software centre.

**X-Road governing authority** – authority, that sets the requirements for using X-Road and establishing the procedure for using X-Road, managing and regulating participants of X-Road.

**X-Road member / member** – participant of X-Road entitled to exchange data/messages on X-Road.

## Trust services

**Approved certification service provider** – Provider of a trust service approved on X-Road, who provides at least following trust services approved on X-Road: service of authentication certificate of Security Server, service of signature certificate of a member, and certificate validation service (OCSP).

**Approved timestamp service provider** – Provider of a trust service approved on X-Road, who provides the timestamp service.

**Authentication certificate of Security Server** – qualified certificate of e-stamp issued by certification service provider approved on X-Road and bound to Security Server, certifying authenticity of Security Server and used for authentication of Security Servers upon establishment of connection between Security Servers. Upon establishment of connection, it is checked from global configuration, if the Security Server trying to establish connection has registered the used authentication certificate in X-Road governing authority (i.e. the used authentication certificate is bound to the ID of Security Server).

**Certification authority (CA)** – is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

**Certification service CA** – is used in the X-Road system as a trust anchor for a certification service. The certification service CA may, but does not have to be a Root CA.

**Certificate signing request (CSR)** – is generated in the Security Server for a certain approved certification authority for signing a public key and associated information.

**Internal TLS certificates** – are used for setting up the TLS connection between the Security Server and the client information systems.

**Signature certificate of a member** – qualified certificate of e-stamp issued by certification service provider approved on X-Road and bound to a member, used for verification of the integrity of mediated messages and association of the member with the message.

**Timestamp** – means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time (EU No 910/2014)

**Timestamping authority (TSA)** – is an entity that issues timestamps. Timestamps are used to prove the existence of certain data before a certain point of time without the possibility that the owner can backdate the timestamps.

**TLS certificate** – is a certificate used by the Security Server to authenticate the information system when HTTPS protocol is used for connections between the service client's or service provider's Security Server and information system.

**Validation service (OCSP)** – Validation service of the validity of certificate issued by certification service provider approved on X-Road.



## Roles of X-Road client

### In terms of dataservice

**Dataservice client** – member of X-Road responsible for using the dataservice in accordance with dataservice usage agreements. Technically, dataservice client is a party of interaction sending the request.

**Dataservice host** – A member enabling access to X-Road services through their information system (as the provider or user of the service) for natural or legal persons, who need not be members of X-Road.

**Dataservice provider** – member of X-Road responsible for dataservice provision, incl. granting the service SLA, managing the agreements with dataservice clients, granting access rights etc. Technically, dataservice provider is a party of interaction sending the response.

### In terms of management of Security

#### Server

**Security Server client** – a member or a subsystem of a member, whose relation with the Security Server is registered in X-Road governing authority and who can use the Security Server on behalf of a member to exchange data on X-Road.

**Security Server host** – a member who provides Security Server hosting services to third parties and other members.

**Security Server owner** – a member responsible for Security Server and creation of a secure data exchange channel.

## X-Road interfacing steps

**Affiliation of membership** – a process ending with becoming a member of X-Road. Becoming a member requires conclusion of affiliation contract and registration of data of the member (name and ID of the member) in X-Road Central Server. Requirements for affiliation are established by X-Road governing authority with relevant regulation/affiliation conditions

**Dataservice interfacing** – a process, where a member of X-Road creates organizational and technical capacity for offering or using dataservice. Interfacing includes development of the service by the member as well as its setup in Security Server, conclusion of service usage contracts and granting access rights. In order to use the service, service provider, as well as service client, shall undergo interfacing.

**Interaction** – activation procedure of dataservice (single use), bilateral information exchange through dataservice, i.e. request of dataservice by the service client by sending a request, to which the service provider will send a response.

**Registration of Security Server** – a process, where organizational and technical capacity of a member of X-Road is created to enable

contacting the information system of the member of X-Road via X-Road. The result is a member of X-Road, with whom a secure data exchange channel of X-Road can be established. To ensure this, at least one Security Server shall be bound to the member in the Central Server.

**Registration of subsystem** – a process for establishing organizational and technical capacity to distinguish organizational users or user groups on the level of a subsystem. Technically, subsystems shall be registered as Security Server clients.

## Elements of X-Road software

### Service and message

**Central service** – dataservice, in case of which the name of service provider is defined by the governing authority. The reason for such alias-name may be the need to assure the service provision (when the service provider changes) without a need to change access rights.

**Dataservice** – web-service executed by a member of X-Road, in order to enable access to the resources of information system of X-Road dataservice provider. The predefined request-response, sent by the information system of a member to the information system of another member and receiving agreed data in response.

**Management service** – services provided by the X-Road governing organization to manage Security Servers and Security Server clients. Management services are implemented as standard X-Road services

following X-Road message protocol.

**Message** – Data set meeting profile description and service description required by X-Road governing authority. Messages are divided into requests and responses. SOAP message consists of headers and a SOAP body that contains service specific content. REST message consists of HTTP verb, path, query parameters, HTTP headers and message body.

**Metadata service** – services between members executed by X-Road governing authority, enabling members of X-Road to get an overview of X-Road (e.g. enabling to get an overview of completed services and access rights needed for the consumption of services). Generally, it shall meet the description of X-Road service.

**Monitoring services** – The X-Road monitoring solution is conceptually split into two parts: environmental and operational monitoring.

- **Environmental monitoring** – is the monitoring of the X-Road environment: details of the Security Servers such as operating system, memory, disk space, CPU load, running processes and installed packages, etc.
- **Operational monitoring** – is the monitoring of operational statistics such as which services have been called, how many times, what is the average response time, etc.
  - **Operational monitoring data** – contains operational data (such as which services have been called, how many times, what was the size of the response, etc.) of the X-Road Security Server(s).
  - **Operational monitoring daemon** – collects and shares operational monitoring data of the X-Road Security Server(s), calculates and shares health data of the X-Road

Security Server(s) that is based on collected operational monitoring data.

**Service client** – is an X-Road member, subsystem, local access rights group or global access rights group that has access rights to one or more services of a Security Server client.

**X-Road service** – SOAP- or REST-based web service or API that is offered by an X-Road member or by a subsystem and that can be used by other X-Road members or subsystems.

## Subsystems and access rights

**Access right** – in X-Road technology enables specifying the rights of Security Server clients (subsystems) to use dataservices.

**Access right group** – set of Security Server clients (subsystems), enabling to grant access rights to the entire group of subsystems and to delegate administration of access rights to the group administrator. Logical name can be assigned to an access right group.

**Global access right group** – access right group administered in the Central Server by the Central Server administrator, usable in the entire X-Road federation.

**Local access right group** – access right group administered in Security Server by Security Server administrator, usable only in the specific Security Server within one Security Server client.

## X-Road protocols

**Federation Protocol** – protocol that is used to distribute configuration between two federated X-Road instances.

**Message protocol** – protocol that is used between information systems and Security Servers in the X-Road system.

**Message Transport Protocol** – communications protocol that is used by service client's and service provider's Security Servers to exchange messages with each other.

**Protocol for Downloading Configuration** – protocol that is used to distribute configuration to Security Servers of an X-Road instance.

**Service Metadata Protocol** – protocol that describes methods that can be used by X-Road participants to discover what services are available to them and download the WSDL files describing these services.

## Logging and security

**Audit log** – log, where the user actions (through user interface), when the user changes the system state or configuration, are logged regardless of whether the outcome was a success or failure.

**Batch signature** – e-stamp provided to a set of documents, enabling to separate a single document from the set and verify its signature.

**Message log** – a log, where exchanged X-Road messages are logged and provided with batch signature. Records all regular messages passing through the Security Server into the database. The messages are stored together with their signatures and signatures are timestamped. The purpose of the message log is to provide means to prove the reception of a request/response message to a third party.

**System service log** – a log which is made from a running system service of a Security Server, for example from xroad-confclient, -proxy, signer services.

## Identifiers and codes

**Central service identifier** – identifier, that uniquely identifies service in X-Road network without having a reference for service provider. Central service identifier consists of X-Road instance identifier and central service code.

**Global access group identifier** – identifier, that uniquely identifies access group in X-Road Network. Global access group identifier consists of X-Road instance identifier and global group code.

**Local access group identifier** – identifier, that uniquely identifies access group for a Security Server client. Global access group identifier consists of X-Road instance identifier and global group code.

**Member class** – identifier, that is identified by the X-Road governing authority and that uniquely identifies members with similar characteristics. All members with the same member class must be

uniquely identifiable by their member codes.

**Member code** – identifier, that uniquely identifies an X-Road member within its member class. The member code remains unchanged during the entire lifetime of the member.

**Member identifier** – identifier, that uniquely identifies a member in the X-Road Network. Member identifier consists of X-Road instance identifier, member class, and member code.

**Security Server code** – identifier, that uniquely identifies the Security Server in all of the Security Servers of the Security Server owner.

**Security Server identifier** – identifier, that uniquely identifies Security Server in X-Road Network. The Security Server identifier consists of Security Server owner identifier and Security Server code.

**Service identifier** – identifier, that uniquely identifies service in X-Road Network. The service identifier consists of member identifier of the service provider, service code and version of the service. Including version of the service in the service identifier is optional.

**Subsystem code** – code, that uniquely identifies subsystem in all of the subsystems of the member.

**Subsystem identifier** – identifier, that uniquely identifies subsystem in X-Road Network. Subsystem identifier consists of member identifier and subsystem code.

**X-Road instance identifier** – identifier, that uniquely identifies the X-Road instance in the X-Road Network.



# Global configuration concepts

**Configuration** – Set of parameters that are distributed by a configuration source. Configuration consists of one or more configuration parts that contain groups of related parameters.

**Configuration Anchor** – is a set of information that can be used by configuration clients to access a configuration source and to verify the downloaded configuration. The configuration anchor is distributed as either a separate XML file in case the anchor points to a local configuration source or as a part of private parameters in case the anchor points to the configuration source managed by a federation partner.

**Configuration Client** – is an entity that uses configuration anchor(s) for downloading configuration from configuration source(s). In an X-Roads system, Security Server and configuration proxy act as configuration clients.

**Configuration part (file)** – is an XML file containing system parameters.

**Configuration Provider** – is an entity responsible for maintaining and distributing global configuration. The configuration provider manages one or two configuration sources through which configuration is made available for configuration clients. In an X-Roads system, the Central Server and the configuration proxy act as configuration providers.

**Configuration Source** – is a component (HTTP server) managed by a configuration provider. The configuration distributed by the source can either be internal configuration or external configuration. The

information needed to access and download configuration from a source is contained in the configuration anchor.

**External configuration** – is distributed by a configuration source and only contains the shared parameters configuration part.

**Global configuration** – a technical solution, through which X-Road governing authority regulates participants of X-Road. Global configuration consists of XML-files, which are downloaded periodically from the Central Server of X-Road governing authority by Security Servers. Global configuration includes following information:

- the addresses and public keys of trust anchors (certification service CAs and time stamping services);
- the public keys of intermediate CAs;
- the addresses and public keys of OCSP services (if not already available through the certificates' *Authority Information Access* extension);
- information about X-Road members and their subsystems;
- the addresses of the members' Security Servers registered in X-Road;
- information about the Security Servers' authentication certificates registered in X-Road;
- information about the Security Servers' clients registered in X-Road;
- information about global access rights groups;
- X-Road system parameters.

**Internal configuration** – is distributed by a configuration source and

is composed of the following configuration parts: private parameters; shared parameters, and; optionally, other configuration parts that are specific to an X-Road instance – optional parameters.

**Monitoring Parameters** – Set of parameters that control monitoring of Security Servers

**Optional parameters** – is an optional configuration part that carries system parameters that have a contextual meaning only to a specific X-Road system installation.

**Private parameters** – is a configuration part that holds system parameters that are only used by Security Servers that are part of the local X-Road system (i.e. the same X-Road system as the Central Server the configuration part originates from). In case of federated X-Road systems, the private parameters contain configuration anchors pointing to configuration sources distributing external configuration of federation partners.

**Shared parameters** – is a configuration part that holds system parameters that are used both by the Security Servers of the local X-Road system and by the Security Servers belonging to X-Road systems federated with the local system.

**Trusted anchor** – is a configuration anchor that points to the external configuration source of a federation partner and has been uploaded to the Central Server during the federation process. Trusted anchors are distributed to the configuration clients of the local X-Road system as a part of private parameters.

# Technical terms

## Trust and security terminology

**CA** - Certification Authority

**HSM** – Hardware security module

**OCSP** – Online Certificate Status Protocol

**SSH** - Secure Shell

**TLS** - Transport Layer Security

**TSA** - Timestamping Authority

**TSP** - Time Stamp Provider

## General software terminology

**API** Application Programming Interface

**CI** - Continuous Integration

**DSL** - Domain Specific Language

**HTTP** - Hypertext Transfer Protocol

**HTTPS** - Hypertext Transfer Protocol Secure

**JMX** - The Java Management Extensions

**JMXMP** - Java Management Extensions Messaging Protocol

**JSON** - JavaScript Object Notation

**MBean** - Java Managed Bean

**MIME** - Multipurpose Internet Mail Extensions

**RPC** – Remote Procedure Call

**REST** - Representational State Transfer

**SDK** - Software Development Kit

**SOAP** - Simple Object Access Protocol

# Implementation models

## Introduction

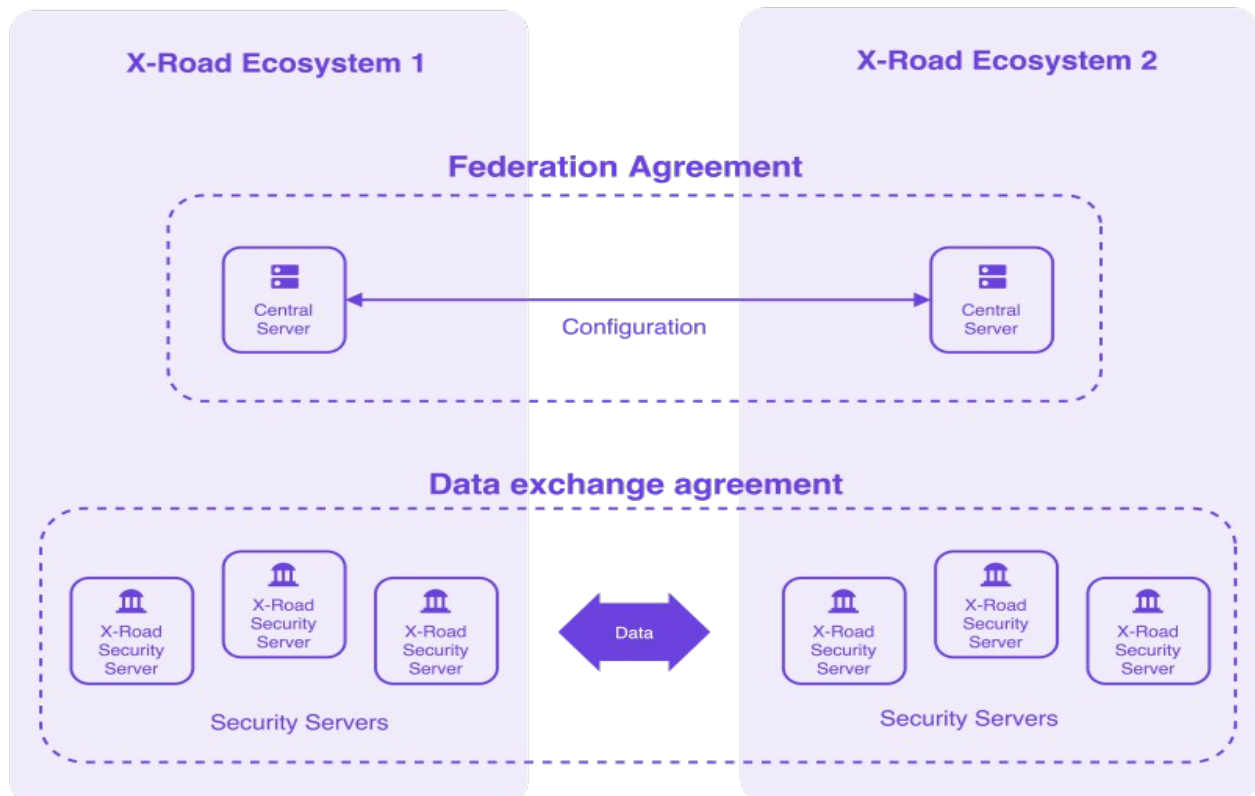
Technically, the X-Road software does not set any limitations to the size of the ecosystem or the member organizations. The ecosystem may be nationwide, or it may be limited to organizations meeting specific criteria, e.g., clients of a commercial service provider. Thanks to its scalable architecture and organizational model, X-Road is exceptionally flexible, and it supports various kinds of setups. Even if a nationwide implementation of X-Road is probably the best known implementation model, X-Road can be used in many other ways too.

## National data exchange layer

National implementation is probably the most typical way to implement X-Road. In a national implementation, X-Road is implemented nationwide within a country, and the aim is to use it in data exchange between organizations across administration sectors and business domains. Typically, the ecosystem is open for all kinds of organizations – both public and private sector organizations. However, it is also possible to restrict the implementation to cover only the public sector, specific administration sector, business domain, or a combination of

these.

Besides, X-Road can be used to implement cross-border data exchange with other countries that have a national X-Road implementation. In practice, the ecosystems of different countries are connected using federation – an X-Road feature that enables connecting two X-Road environments. Federation enables member organizations of different ecosystems to exchange data as if they were members of the same ecosystem.



In a national implementation, a government agency is usually the owner of the ecosystem. The owner takes the role of the X-Road operator, who is responsible for all the aspects of the operations. The responsibilities include defining regulations and practices, accepting new members, providing support for members, and operating the central

components of the X-Road software. Technical activities can be outsourced to a third party, but administrative and supervising responsibilities are carried out by the operator.

There are multiple implementations around the world where X-Road is used as a national data exchange layer. The best known national X-Road ecosystems are in [Iceland](#), [Finland](#), and [Estonia](#).

## Data exchange solution for regions

Regional implementation means implementing X-Road within a region or an autonomous community, such as a region, a province, or a state. In a regional implementation, X-Road is used within a region, and the scope is usually very similar to the national implementation – data exchange between organisations across administration sectors and business domains. However, the scope may be more restricted, as well. Besides, X-Road may be used to exchange data with the central government and/or other regions.

In a regional implementation, a regional agency or authority is usually the owner of the ecosystem. The owner takes the role of the X-Road operator, who is responsible for all the aspects of the operations. Some of the technical activities may be outsourced, just like in the national implementation.

As an alternative approach, the national implementation described earlier may consist of multiple regional implementations too. Every region or some of the regions within a country can have their X-Road



ecosystems that are connected using federation. However, compared to a single national implementation, this approach generates more overhead since every region must manage and operate its X-Road ecosystem. Therefore, when targeting for national implementation, a single national ecosystem is recommended over multiple regional ecosystems that are connected using federation.

One example of a regional implementation can be found from Argentina. The [province of Neuquén](#) in Argentina is using X-Road as a regional data exchange platform. Also, some regions in other countries are currently considering the use of X-Road on a local level.

## **Data exchange within a business domain or sector**

In national and regional applications, X-Road is implemented within a geographic area, such as a country or a region. However, there are no restrictions on why an X-Road ecosystem could not span multiple states and/or regions as long as there's an organisation that takes the role and responsibilities of the X-Road operator. A practical example of this kind of approach is implementing X-Road within a business domain or sector in which members are located in different countries around the world. However, X-Road could be implemented within a business domain or sector on the national level too.

The critical factor is that all members commit to follow the rules and policies of the ecosystem set by the X-Road operator. In this case, the use of X-Road is based on a mutual agreement between the members of

the ecosystem. In national and regional implementations, the use of X-Road is often based on a law or a regulation issued by a governmental or regional authority.

In case different business domains have their X-Road ecosystems, they can be connected using federation, which enables data exchange between member organisations of different business domains. Technically, a business domain-specific implementation can be connected to a national or regional X-Road ecosystem too.

X-Road based business domain-specific solutions have been implemented in several countries. For example, in [Germany](#) X-Road is being used to exchange healthcare data, and in [Estonia](#), the X-Road based Estfeed platform is utilised in energy sector data exchange. Besides, Estfeed is also applied by the [Data Bridge Alliance](#) to exchange energy data on a cross-border level.

## **A platform for data exchange within an organisation**

The primary use case for X-Road is data exchange between organisations, but there are no restrictions on why X-Road could not be used to exchange data within an organisation too. For example, a large international organisation that has branches and departments in different countries and continents may have information systems that

communicate over the public Internet. X-Road provides a solution to connect those systems in a standardised and secure manner guaranteeing confidentiality, integrity, and interoperability of the data exchange.

When it comes to the organisational model of X-Road, one of the departments takes the role of the X-Road operator, and other branches and departments are members of the ecosystem. In addition to connecting information systems communicating over the Internet, X-Road could be used inside a private network of an organisation too.

One example of corporate use of X-Road can be found in Japan. A major [Japanese gas company](#) uses an X-Road based solution to exchange data between its different organisation units. Another interesting approach to corporate use is building a commercial product on top of X-Road. Since X-Road is open source and licensed under the permissive MIT license, it can be utilised in commercial closed source products too. For example, Planetway, a Japanese-Estonian company, has built its [PlanetCross](#) platform using X-Road.

For clarity, X-Road is not a service mesh platform for microservices, such as [Istio](#). X-Road is meant for data exchange between information systems over the public Internet, and service mesh platforms are used as a communication layer between different microservices in a microservices architecture. The high-level capabilities that X-Road and many service mesh solutions provide may seem very similar. Still, the way how they have been implemented is optimised for very different use cases. Therefore, [X-Road is not to be mixed](#) with service mesh solutions.

# Architecture

## Introduction

### Overview

X-Road is a system for enabling secure communication between organizations. This document 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.

### Design Goals

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.

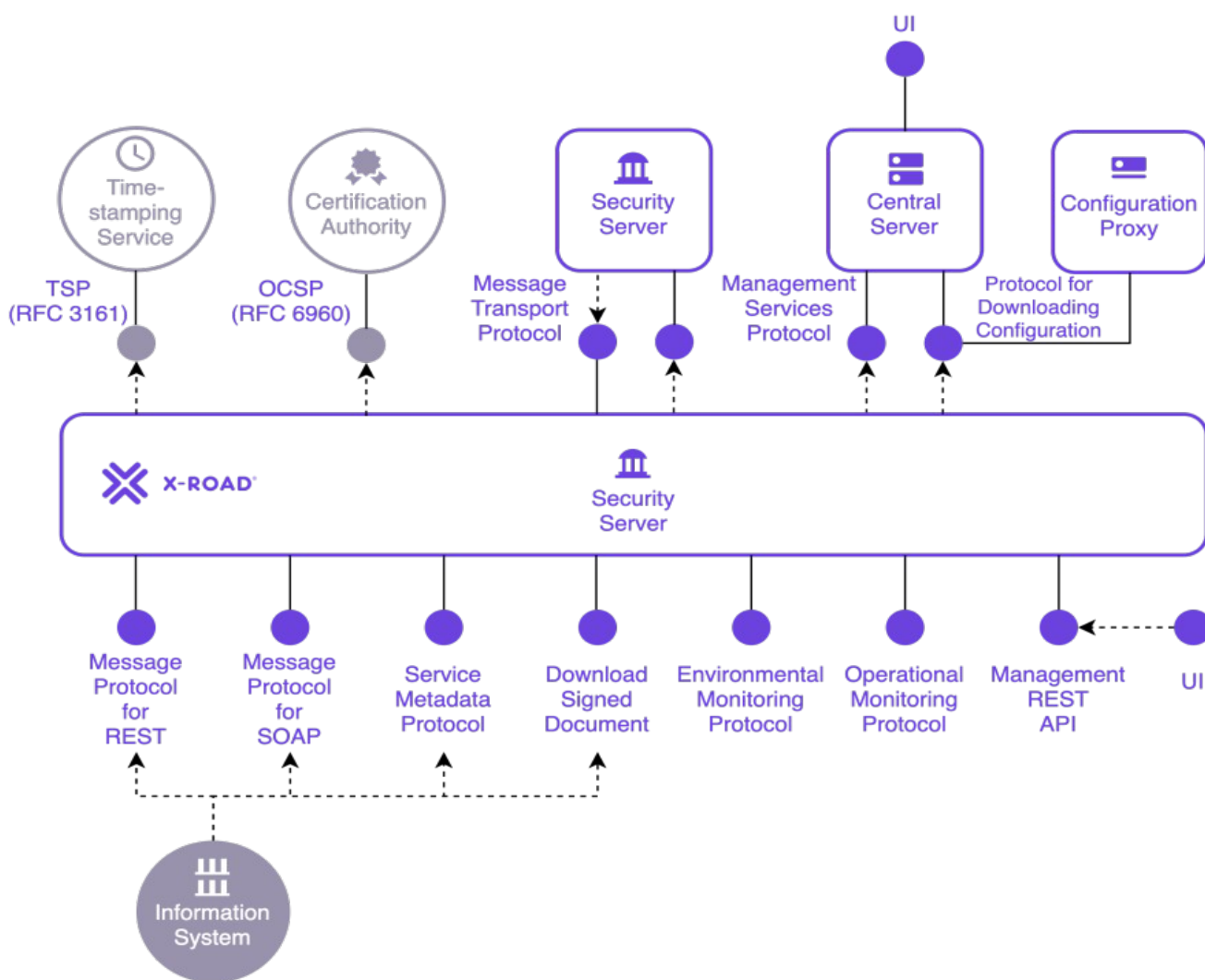
The data owner (service provider) controls who can access particular services.

- **Availability** is a central concern – 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 SOAP or REST **service calls**. SOAP services are described using the WSDL language and REST services are described using the OPENAPI Specification v3.
- **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.

# System components

Figure 1 shows the main components and interfaces of the X-Road system. The components that are not part of the X-Road core are marked with grey color. The components and the interfaces are described in detail in the following sections.



## 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.

## Security Server

The Security Server 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 message protocol for SOAP and a message protocol for REST. The protocols are 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.

## 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 an 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 service request. 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 or a REST service and makes it available over the X-Road. For this purpose, the service must conform to the X-Road message protocol for SOAP or message protocol for REST. A SOAP service must be accompanied by a WSDL service description, and a REST service may be accompanied by an OpenAPI Specification v3.

## Time-Stamping Authority

The time-stamping authority issues time stamps that certify the existence of data items at a certain point of time. The time-stamping authority must implement the time-stamping protocol described in the following lessons.

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.

## 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.

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.

## 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.

## 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.

## Environmental Monitoring Daemon

The environmental monitoring daemon gathers information about the Security Server's operating environment and makes it available for external monitoring systems via corresponding interfaces.

## Protocols and interfaces

### 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.

X-Road provides a message protocol for SOAP and a message protocol for REST. The X-Road Message Protocols are based on SOAP/REST over HTTP(S) and adds additional header fields for identifying the service client and the invoked service.

These protocols (together with the Message Transport Protocol) form 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.

## 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.

## 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/REST 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.

## 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.

## 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.

## 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).

## 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.

## 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 vary between different instances of X-Road.

## **Security Server User Interface**

The Security Server user interface is used by the Security Server administrator to configure and manage the Security Server.

## **Central Server User Interface**

The Central Server user interface is used by the Central Server administrator to configure and manage the Central Server.

## **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).

## **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.

## **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.

## **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.

## **Environmental Monitoring Protocol**

The environmental monitoring interface responds to queries for monitoring environmental data from Security Server's serverproxy interface. The environmental monitoring data is collected by environmental monitoring service.

## **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.

## **Environmental Monitoring Query**

The environmental monitoring query interface is used by the X-Road Security Server to retrieve environmental monitoring data from the

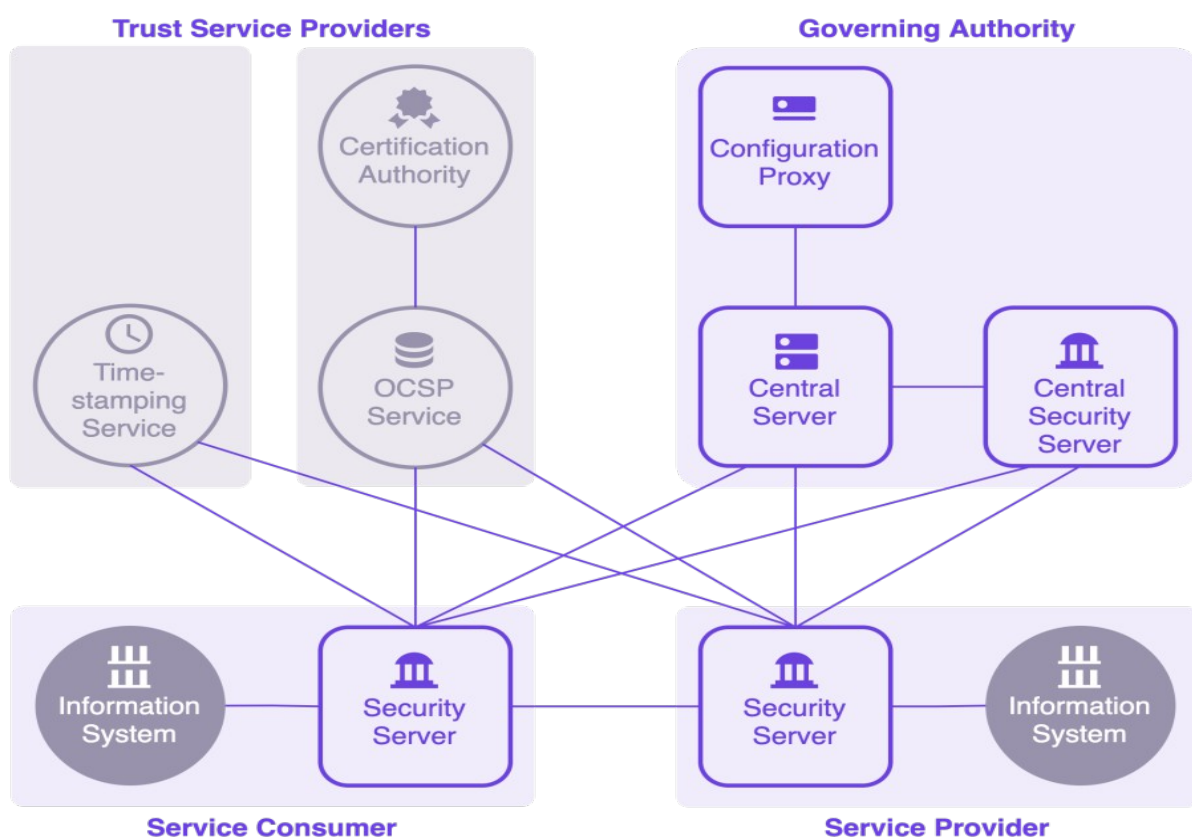
environmental monitoring daemon.



## Deployment view

Figure 1 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 consumer and service provider organizations host their information system and Security Server that connects the information system to the X-Road.



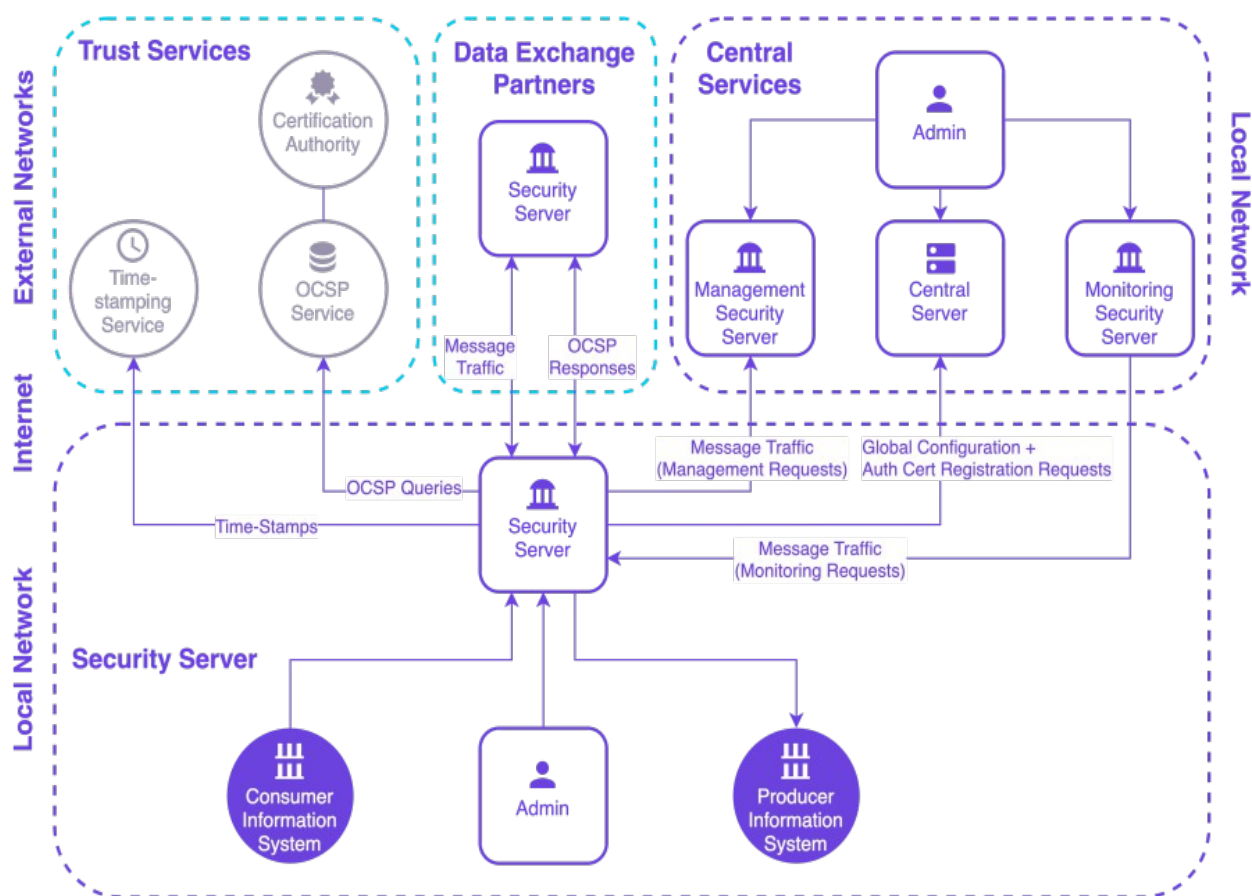
# Security Architecture

## Introduction

X-Road is an open source data exchange layer solution that enables organizations to exchange information over the Internet. X-Road is a centrally managed distributed data exchange layer between information systems that provides a standardized and secure way to produce and consume services.

This document describes the X-Road security architecture and how it fulfills security and privacy principles and best practices. Technical descriptions and guides for X-Road components and protocols are found in separate documents.

Figure 1 X-Road Security Architecture depicts the X-Road environment and its actors and the data exchanges between them.



The identity of each organization (X-Road Service Provider or Service Consumer) and technical entry point (Security Server) is verified using certificates that are issued by a trusted Certification Authority (CA) when an organization joins an X-Road ecosystem. The identities are maintained centrally, but all the data is exchanged directly between a consumer and provider. Message routing is based on organization and service level identifiers that are mapped to physical network locations of the services by X-Road. All the evidence regarding data exchange is stored locally by the data exchange parties, and no third parties have access to the data. Time-stamping and digital signature together guarantee non-repudiation of the data sent via X-Road.

## Environment Assumptions

X-Road facilitates a data bridge infrastructure between a variety of organisational actors, such as government registers, financial institutions, and telecommunications service providers. X-Road is therefore a critical information infrastructure (CII) system essential for the operation and sustainability of data exchange between such X-Road member organisations. Disruption of CII may be caused by a variety of human-induced actions or technical failures.

X-Road security is therefore designed with CII-equivalence resilience in mind. Organisations must register with and be affiliated to X-Road, and acquire identity and signing certificates and keys, before they can perform data exchange.

## Confidentiality

For compliance with the security principle of confidentiality, the objective is to limit visibility of X-Road assets (organisational data) to the actors (registered X-Road organisational members) that are authenticated and authorised to see the data. With assurance of confidentiality, the threat being mitigated is the unintended revealing of X-Road assets to unauthorised third parties.

X-Road messages transmitted over the public Internet are secured using digital signatures and encryption. The motivation for bidirectional HTTP over Transport Layer Security (TLS) is to enforce anti-eavesdropping and anti-tampering protections to ensure the integrity and privacy of the messages exchanged between X-Road actors. X-Road-internal TLS certificates are used for setting up the TLS connection between the



Security Server and information systems that provide and consume services.

## Integrity

For compliance with the security principle of integrity, the objective is to ensure that X-Road assets are not modified and do not become corrupted. With assurance of integrity, the threat being mitigated is unauthorised access to and unauthorised actions upon X-Road assets.

X-Road incorporates a public key infrastructure (PKI) whereby a certification authority (CA) issues authentication certificates to Security Servers and signing certificates to X-Road member organisations. The CA processes certificate signing requests conforming to PKCS10.

All X-Road messages are signed by the signing key of the organisations that send the messages and all messages are logged. Message logging is enabled by default. This means that both message headers and message bodies are logged. Logging of message bodies may be disabled on Security Server level or for selected subsystems. The logs are stored as plaintext on the Security Server.

## Availability

For compliance with the security principle of availability, the objective is to ensure that X-Road assets are readily available to authorised X-Road actors that require them. With assurance of availability, the threat being mitigated is the denial to authorised actors of X-Road services.

Availability is a cornerstone of critical infrastructure. X-Road is designed so that no component is a system-wide bottleneck or point of failure.

Security Servers remain operational even if Central Server, OCSP service and/or time-stamping service would fail. The grace period depends on the failing component and configuration of the X-Road instance.

X-Road Security Servers incorporate denial-of-service mitigation functionality. X-Road Linux services will automatically restart after a local system crash.

To fortify the availability of the entire X-Road system, the service consumer's/user's and service provider's Security Servers may be set up in a redundant configuration as follows:

- One service user can use multiple Security Servers in parallel to perform requests.
- If a service provider connects multiple Security Servers to the network to provide the same services, the requests are load-balanced amongst the Security Servers.
- If one of the service provider's Security Servers goes offline, the requests are automatically redirected to other available Security Servers.

# Authentication and access control

## Authentication

For compliance with the security principle of authentication, the objective is to ensure that the provenance (identity) of the X-Road asset or X-Road actor is known and verified. This is accomplished in a standardised manner using authentication keys and certificates. With assurance of integrity, the threat being mitigated is unauthorised access to X-Road infrastructure and assets therein.

X-Road enforces organisation-level authentication (and authorization) mechanisms and for X-Road Administrator web application frontend-to-backend connections and direct calls to the backend for configuration and maintenance automation purposes.

An X-Road organisation's client information system Security Server acts as the entry point to all the X-Road services. The client information system is responsible for implementing an end user authentication and access control mechanism that complies with the requirements of the particular X-Road instance. The identity of the end user may be made available to the service provider by including it in the service request.

In case a Security Server becomes compromised, it can be blocked from the X-Road instance by revoking its authentication certificate or removing it from the Central Server's configuration. Similarly, a selected member organisation or subsystem can be blocked out centrally without

affecting other Security Servers, members or subsystems.

## Access Control

For compliance with the security principle of least privilege, the objective is to ensure that X-Road actors, processes and controls must be able to access only the X-Road information and resources that are limited to and necessary for the legitimate and intended purpose.

## Messaging Access Control

X-Road core handles access control on the organisation level during data exchange between registered X-Road members. A service provider is responsible for managing access rights to its services. Publishing services via X-Road does not automatically provide other members access to the services.

## Web UI Access Control

When the end user is successfully authenticated, least privilege-based access control is enforced for access to system resources whereby the frontend receives information about current user's roles and permissions using /api/user resource. The backend defines authorisation rules based on permissions.

Details on Security Server user roles and associated access controls are described in section 15.1 Security Server Roles.

In X-Road, access control starts by denying all access by default. Access will not be allowed to all roles if a new resource is added and authorisation is somehow configured incorrectly.

# Input validation and logging

## Input Validation

For compliance with the principle of sanitised input, it is security best practice to validate all inputs at the server. X-Road has two validation aspects; a) web UI input validation and b) messaging validation.

### Web UI Input Validation

User input parsing is enforced in the Central Server UI and the Security Server UI, whereby there is removal of leading and trailing whitespaces, verification that all mandatory fields are filled, and verification that the user input does not exceed 255 characters.

If one or more mandatory fields are not filled, it results in a "Missing parameter: 'X'" error message. If user input exceeds 255 characters, it results in a "Parameter 'X' input exceeds 255 characters" error message.

### Messaging Validation

When input contains XML, it must be validated against its schema before using it. XML injection attacks are mitigated by ensuring that XML input follows the rules specified in the schema. Down-stream errors that might be caused from invalid XML input are mitigated by validating the XML at the earliest point where it crosses a trust boundary.

## Logging

For compliance with the security principle of non-repudiation, all messages processed by X-Road are usable as digital evidence. The technical solution complies with requirements for digital seals according to regulation for electronic identification and trust services for electronic transactions (EIDAS). EIDAS defines two levels for digital seals: 1) advanced and 2) qualified. Qualified digital seals require that a hardware security module (HSM) device must be used for storing private keys and the CA issuing the certificates must be present in the EU's list of trusted trust service providers. X-Road supports HSMs and X-Road operators can choose the CAs that are used in their environments. If these requirements are not met, then the digital seals created by X-Road are advanced instead of qualified.

X-Road incorporates the following logs:

- **Audit log** – log where user-configured changes to the system state or configuration (via the user interface) are logged, regardless of whether the outcome was a success or failure.
- **Message log** – provides the means to prove the reception of a regular request or response message to a third party. Messages exchanged between Security Servers are signed and encrypted. For every regular request and response, the Security Server produces a complete signed and timestamped document. Messages are logged and provided with a batch signature. The purpose of the message log is to provide the means to prove to a third party the reception of a request/response message. The Security Server message log saves each request and response message sent through the Security Server to the message log

database. There is one log record inserted per transaction. Periodically (by default every six hours), the log archiver reads all non-archived records from the database, writes them to disk, and updates the records in the database, marking them as archived. Every twelve hours, the log cleaner executes a bulk delete removal of all archived records that are older than a configurable age; the default is thirty days. Message archiving interval lengths are configurable via configuration settings. The Security Server administrator is responsible for transferring the archived log files into long term storage. Such storage components are organisation-specific.

- **System service log** – log which is made from a running system service of a Security Server, for example from xroad-confclient, -proxy, signer services.

If a message log audit is required, message logs for some time period may be queried; this creates a zip file that contains the logs in a tamper-resistant format (signed hash of the log tree).

# Time-stamping and updatability

## Time-Stamping

Also related to the security principle of non-repudiation (and integrity), a time-stamping authority enforces use of a time-stamping protocol by Security Servers to ensure long-term proof value of exchanged messages. The issued time stamps certify the existence of the messages at a certain point of time and the Security Servers log all of the messages and their signatures. These logs are periodically time-stamped to create long-term proof.

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, rather it depends on the number of Security Servers in the system.

X-Road supports creating time-stamps synchronously for each message too. Using synchronous time-stamping may be a security policy requirement to guarantee the time-stamp at the time of logging the message. However, batch time-stamping is the default for performance and availability reasons.

## Updatability

X-Road is designed to enable reliable installation of software updates



including security updates. X-Road software packages are signed so that their origins are traceable.

## Trust federation

The trust federation of X-Road instances allows for the members of one X-Road instance to use the services provided by members of the other instance, thus making the X-Road systems interoperable.

To make the federating systems aware of each other, the external configuration anchor of the federation partner must be uploaded as a trusted anchor to the Central Servers of the federating X-Road instances.

The trusted anchors are distributed to the Security Servers as a part of the internal configuration. The Security Servers use the trusted anchors to download external configuration from the federation partners. The external configuration contains the information that the Security Servers of the partner instances need to communicate with each other.

To end a federation relationship with an X-Road instance, the trusted anchor of that instance must be deleted from the Central Server.

## Standardised protocols

For compliance with security principle of economy of mechanism, X-Road member organizations are not required to implement security-dependent methods for data exchange; they are able to connect to any number of service providers via the following standardized protocols that ensure security-supportive functional consistency. Summaries of the protocols are as follows:

- Message Protocol is used by service client and service provider information systems for communicating with the X-Road Security Server.
- Message Transport Protocol is used by Security Server to exchange service requests and service responses. The protocol is based on HTTPS and uses mutual certificate-based TLS authentication.
- Configuration Download Protocol is a synchronous protocol that is offered by the Central Server. Configuration clients download the generated global configuration files from the Central Server. It is used by configuration clients such as Security Servers and configuration proxies.
- Service Metadata Protocol may be used by the service client information systems to gather information about the X-Road instance and may be used to find X-Road members.
- Download Signed Document Protocol may 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

may be used to verify the signed containers.

- Management Services Protocol is used by Security Servers to perform management tasks such as registering a Security Server client or deleting an authentication certificate. 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 is implemented directly by the Central Server.
- Online Certificate Status Protocol (OCSP) is used by the Security Servers to query the validity information about the signing and authentication certificates. OCSP protocol is a 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 to ensure that the Security Servers do not need to discover the OCSP service used by the other party.
- Time-Stamping Protocol is used by Security Servers to ensure long-term proof value of exchanged messages. The Security Servers log all messages and their signatures. These logs are periodically time-stamped to create long-term proof. Time-stamping is used in an asynchronous manner, so temporary unavailability of the time-stamping service does not directly affect the X-Road message exchange.

# Central Server and Security Server

## Central Server

The 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:

- list of trusted certification authorities,
- list of trusted time-stamping authorities,
- tuneable 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 the HTTP protocol. This distributed set of data forms the global configuration. The integrity of the global configuration is guaranteed using digital signatures - the Central Server signs the global configuration, and the signature is verified by the Security Servers.

The set of information that is needed to access the configuration source and to verify the downloaded global configuration is distributed to the Security Servers using the configuration anchor. The configuration anchor is an XML file, and it is uploaded to the Security Server by the Security Server administrator during the initialization process. The X-Road operator is responsible for providing the configuration anchor to the new member organisations.

## Security Server

The main function of a Security Server is to mediate requests in a way that preserves their evidential value. The Security Server is connected to the public Internet from one side and to the information system within the organization's internal network from the other side (refer to Figure 1 X-Road Security Architecture). The Security Server is equipped with the functionality required to secure the message exchange between a client and a service provider.

A Security Server instance is an independent and separately identifiable entity. A Security Server identity consist of a server identifier (member id + server code). For each server identifier there may be multiple authentication certificates present locally, each of which must be unique. However, only one authentication certificate must be active and registered on the Central Server at a time. In addition, each Security Server has an address (DNS name or IP address) which is not required to be unique. The global configuration binds together the authentication certificate(s), server identifier and address. The authentication certificate may contain information about the service identifier; however this is optional. Also, the server address and the common name or alternate subject names in the authentication certificate may be different.

Messages transmitted over the public Internet are secured using digital signatures and TLS (HTTPS) encryption. On every connection, the Security Server verifies that the authentication certificate of the other Security Server:

- is issued by an approved certification authority
- matches the authentication certificate registered to the Security

Server on the global configuration

- has a valid OCSP response available.

If any of the above verifications fail, the message is not processed further and an error message is returned.

The service provider's Security Server applies access control to incoming messages, thus ensuring that only those X-Road members (consumer information systems) that have been explicitly allowed access can access a service. Managing access rights of a service is the responsibility of the administrator of the service provider's Security Server.

## Certificates and key management

Only certificates issued by approved certification authorities can be used in X-Road. Approved certification authorities are defined on the Central Server and the configuration is environment specific. It is possible to have multiple approved certification authorities within an X-Road instance.

Security Server authentication key and certificate are stored on a software token. Central Server and Security Server signing keys and certificates can be stored on a software token or an HSM device.

The signer component is responsible for managing signing keys and certificates. The signer is called by other components when creating or verifying signatures. The user interface also calls the signer when

generating authentication and signing keys or certificate requests.

By default, X-Road utilises 2048 bit RSA keys as authentication and signing keys/certificates. The key length may be configured using the Security Server system parameters. Longer keys may be utilised in X-Road without compatibility issues; 2k, 3k and 4k keys may be simultaneously utilised.

## Monitoring

## Monitoring

X-Road monitoring is conceptually split into environmental and operational monitoring.

### Environmental Monitoring

Environmental monitoring provides details of the Security Servers such as operating system, memory, disk space, CPU load, running processes, installed packages, X-Road version information etc.

It is possible to limit the environmental monitoring data set that is returned to the central monitoring client. The limited data set includes certificate, operating system and X-Road version information.

## Operational Monitoring

Operational monitoring collects data about request exchange between Security Servers. The data includes, but is not limited to:

- ID-s of the client and the service
- various attributes of the message read from the message header
- request and response timestamps
- message size and processing time

## Controlling Access to Monitoring

Both environmental and operational monitoring queries are allowed from

- a client that is the owner of the Security Server
- a central monitoring client (if any have been configured)

In addition, a regular client is allowed to query its own operational monitoring records - records that are associated with the client sending the query.

The central monitoring client is configured via Central Server administrator user interface. Attempts to query monitoring data from other clients results in an AccessDenied system response.



# Privacy and regulatory compliance

## Privacy

Security best practice supports and facilitates privacy best practice. Privacy involves Personally Identifiable Information (PII) which is any data (including IP addresses) that allow the identification of a person, any data that the person has disclosed to an X-Road operator, or the person's or other person's data that are in their possession, including Personal data.

X-Road is obligated to comply with the General Protection Data Regulation (GDPR) that stipulates how personal data must be processed in any operation performed on personal data, including collection, recording, organization, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage, combination, closure, erasure, destruction, or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used.

When GDPR (or any other rule/regulation) must be applied, an X-Road member organisation is responsible for maintaining and operating its Security Server(s) in a manner that is compliant with the rule/regulation.

## Purpose Limitation

X-Road data is communicated, processed and stored only for the specified, explicit and legitimate intended purposes and not in any manner that is incompatible with X-Road data purposes and X-Road security policy.

X-Road data purposes and X-Road security policy are member organisation and X-Road instance specific, and they may be influenced by local interpretations of both national and international legislation.

## Data Minimisation

X-Road data is limited to what is adequate, relevant and necessary in relation to the purposes for which data are processed.

## Regulatory Compliance

X-Road is obligated to comply with security requirements stipulated by the following regulatory bodies:

### Common Regulations

Common European Union (EU) regulations:

- EIDAS – 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.
- GDPR – General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data.

## **Environment and Country-Specific Regulations**

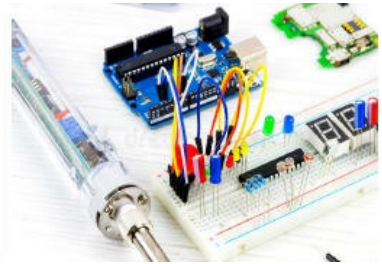
Environment and country-specific regulations:

- VAHTI – Information security standard that is developed for the Finnish public sector. VAHTI is compulsory for Finnish state and local government organisations who handle databases/registers.
- ISKE - Information security standard that is developed for the Estonian public sector. ISKE is compulsory for Estonian state and local government organisations who handle databases/registers.

Course: EE02000  
**AUTOMATION and ELECTRONICS  
TECHNICIAN**



Course: EEE0120  
**Electronics with  
Microcontrollers Programming**



Course: EEE0100  
**ELECTRONICS  
TECHNICIAN**



Course: EE01000  
**ELECTRICIAN  
TECHNICIAN**



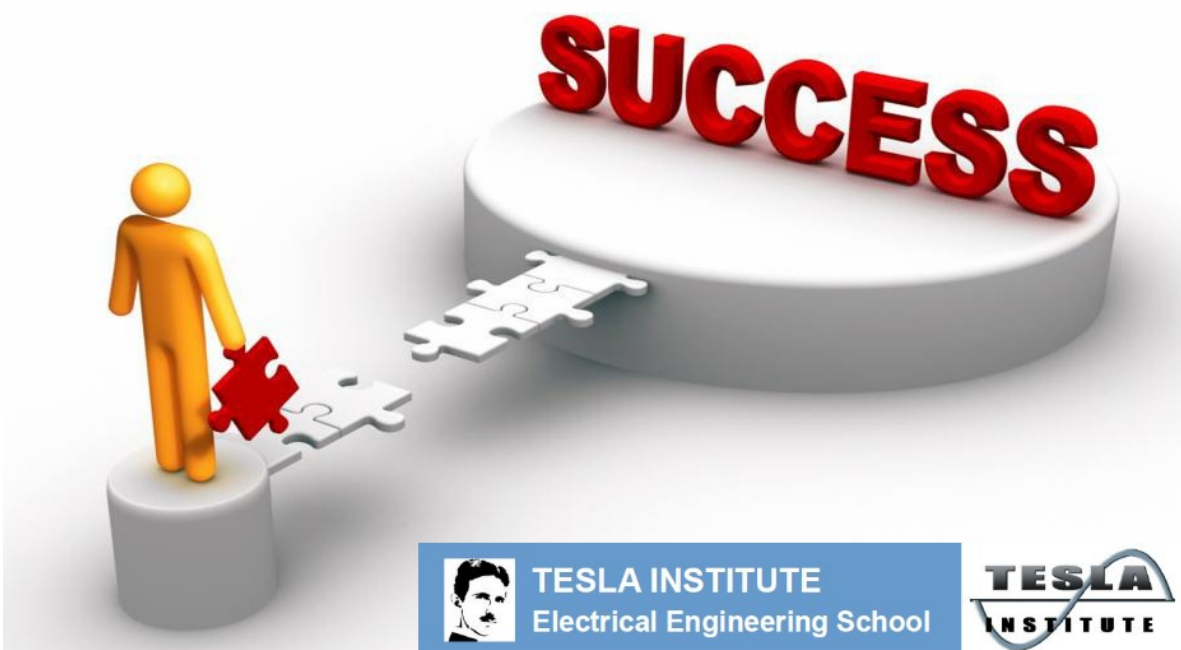
Course: CT01000  
**COMPUTER TECHNOLOGY  
TECHNICIAN**




Course: EEE0130  
**Microcontrollers Programming**



Course: EE02100  
**Introduction to Programmable Logic Controllers (PLC)**



**TESLA INSTITUTE**  
Electrical Engineering School



## Like TESLA INSTITUTE Page



## Subscribe our Youtube channel



## Learn more with Young English Engineer

