Federating X-Road System Overview

Frozan Maqsoodi
Institute of Computer Science,
University of Tartu
frozan.maqsoodi@ut.ee

I. ABSTRACT

X-Road is a secure Internet based data exchange system used in Estonian public and private organizations. It is a middleware originally developed in Estonia in early 2000s. This report includes how X-Road system can be used in cross-border communication and the components and architectures used to establish the cross-border communication system with X-Road.

II. INTRODUCTION

X-Road is a system that ensures secure and direct data exchange between its members. All the members in the X-Road data exchange are ensured with anatomy (i.e rendering services through X-Road and giving the right access to use the services), confidentiality (only authorized parties should be able to receive any information), evidential value (usage of digital signature to prove the source of received data), and interoperability (all X-Road members speak the same language, regardless of the technology or architecture a member is using) [10]. The main purpose of using X-Road system is that it allows the de facto data exchange standard in the public sector of Estonia. It offers a uniform, cost-effective and high security to all exchanged data: confidentiality, uniformity, evident value and minimum impact on availability.

The X-Road system is the backbone of the Estonian State because the absolute majority of registers and databases kept by the Estonian State are made available via X-Road. To enhance it usage, the Estonian Information System Authority initiated a project that supported cross-border services. This project goal is to develop the capability of facilitating cross-border e-services. The scope of this project was to exchange cross-border e-services with seven foreign countries in which Finland is one of the main stakeholders. [1] This paper is a summary of the X-Road system analysis conducted in 2015. The analysis was implemented in two phases. First, an initial analysis was carried to find the technical and procedural solutions for supporting cross-border services in X-Road system. Second, the result of the initial analysis was presented to Estonian Information System Authority for evaluation and used for specification of the scope of the system under development. [2] In addition, the analysis phase creates some artifacts such as business use case model and user interface designs, which were further detailed with system components data models.

Without the X-Road system, the state might have used a central super database to store and exchange its data across Estonia. The X-Road development was built on three core tenants of information security: data availability, data integrity, and data confidentiality. Considering these factors, the X-Road system was launched in 2001 and by the end of 2016, the X-Road system had 1789 connected services by 246 service providers. More than 2000 of X-Road services were used and provided by public registers and databases. Collectively, 975 member organizations exchanged roughly 575 million transactions per year. The development of next generation of X-Road began in 2014, which was based on product prototype. The aim behind the next development phase was international deployment and cross-border electronic services. The X-Road production in Estonia is version 5. The Estonian Information System Authority in collaboration with Cybernetica AS, Estonian eHealth Foundation, the Finnish Government and other partners, has been developing the next generation of the system X-Road version 6. Since version 6 is not backward compatible with X-Road version 5, a transitional version of X-Road system - version 5.5 is developed in parallel to version 6 to facilitate the transition from version 5 to version 6 in Estonia [1]. Version 6 will support new functionality such as the capability for supporting cross-border exchange. The main objective of the development of X-Road system supporting cross-border services is to develop a solution for a network of X-Road systems situated in different countries exchanging cross-border services. This project is implemented to establish and create trust federation between X-Road system users.

The paper is structured in the following ways: Section III describes briefly the X-Road infrastructure. Section IV describes the architecture. Section V discusses the X-Road Components for federation exchange system. Section VI discusses the X-Road federation and federation requirements. Section VII is the analysis conducted on the main components for developing X-Road cross-border.

III. X-ROAD INFRASTRUCTURE

Fig 1 presents a concise view of X-Road architecture. The X-Road installation is managed by a Governing Authority, which is responsible for all data exchange policies and

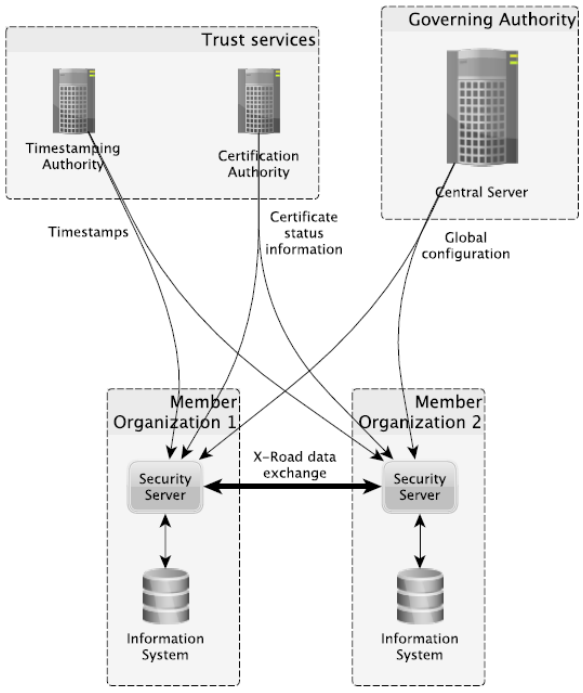

Fig. 1. X-Road infrastructure

determining legal status in the data exchange. The Governing Authority also sets up and maintains the central server, which contains member directory and other data. The communication over X-Road is digitally signed to ensure integrity. This is possible through a proper public key infrastructure (PKI). PKI requires two main components: certification authority and timestamping authority. The trusted PKI service providers list are specified by the Governing Authority and this list is made available for global configuration as well. The X-Road member organizations in the interoperability layer communicate directly for data transfer with each other. The communication is a synchronous structured call. All messages that are exchanged are validated by timestamping and signing. X-Road uses security servers as a standard component for implementing a well security measure in all its organization. This standard encapsulates the security protocol and ensures proper implementation, which also acts as a gateway between its member organizations. The data exchange occurs directly between the security servers of each member organization, this decentralized system is governed by the Governing Authority, which defines, distributes, and enforces all policies for the whole system.[2]

IV. X-Road Architecture

The X-Road is a distributed, secure, unified web-services based inter-organizational data exchange framework [1]. During its design, the following principles were followed:

- Distributed architecture: X-Road system has distributed management. The data on X-Road is not centralized and data ownership remains unchanged.
- Heterogeneous integration: X-Road connects any information system independent of their IT platform and does not prescribe any tools and technologies for intra-organizational use.
- End-to-end confidentiality: the participants of the X-Road communicate directly with each other. The messages are encrypted at the endpoints and are not visible to any external parties.
- Authentication and non-repudiation: the request and responses messages are signed by the originating entity using a qualified certificate. All the signed messages are timestamped and logged to verify the validity of the signature at a later date.
- Reliability:the system does not have a single point of failure. The system components are made redundant for high resiliency against failures and attacks [1].
- Based on open standards: X-Road is based on open standards such as HTTP [2], SOAP[4], WSDL[5], MIME [6], X.509[7], TLS[8], RFC3161, and RFC6960 [9].

V. X-Road Federation

Federating X-Road installations was first studied by Ansper and Willemson in 2008 [11]. The following strategies were proposed:

1) A new higher level is defined having all the present X-Road infrastructures as its descendants
2) To facilitate international queries, a new cross-border X-Road instance is established in parallel with the existing ones.
3) All nations have their own X-Road infrastructures, and no additional ones are defined. A bilateral agreement are made between the existing governing institution to allow international information exchange. The X-Road federation infrastructure is depicted in Fig 2. As shown in the figure, the two governing authorities enter a bilateral agreement. They exchange the configuration anchors pointing to their respective shared parameters file. X-Road uses a public key infrastructure so that each security server only interacts with the Certification Authority that issued its own certificate. Every time a security server receives a certificate, it comes with all necessary information needed to verify it [11]

A. X-Road Federation Requirements

The public procurement stated the following requirements for developing the federation-capability for the X-Road system.

- The solution for cross-border services cannot require changes in the structure or functionality of X-Road services
- Use of cross-border services cannot add an additional requirement to the X-Road members.
- Federation must be bilateral- the federation agreement has two counterparts.
- X-Road system retains it autonomy when entering into a federation relationship. Governing agencies of the

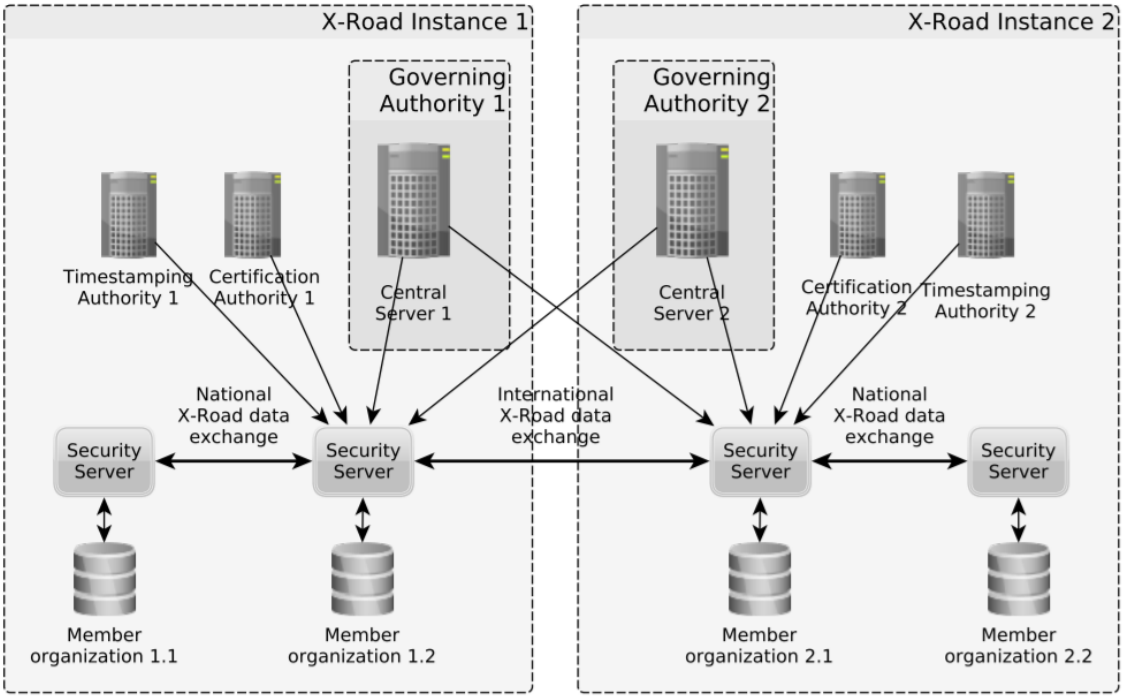

Fig. 2. X-Road Federation

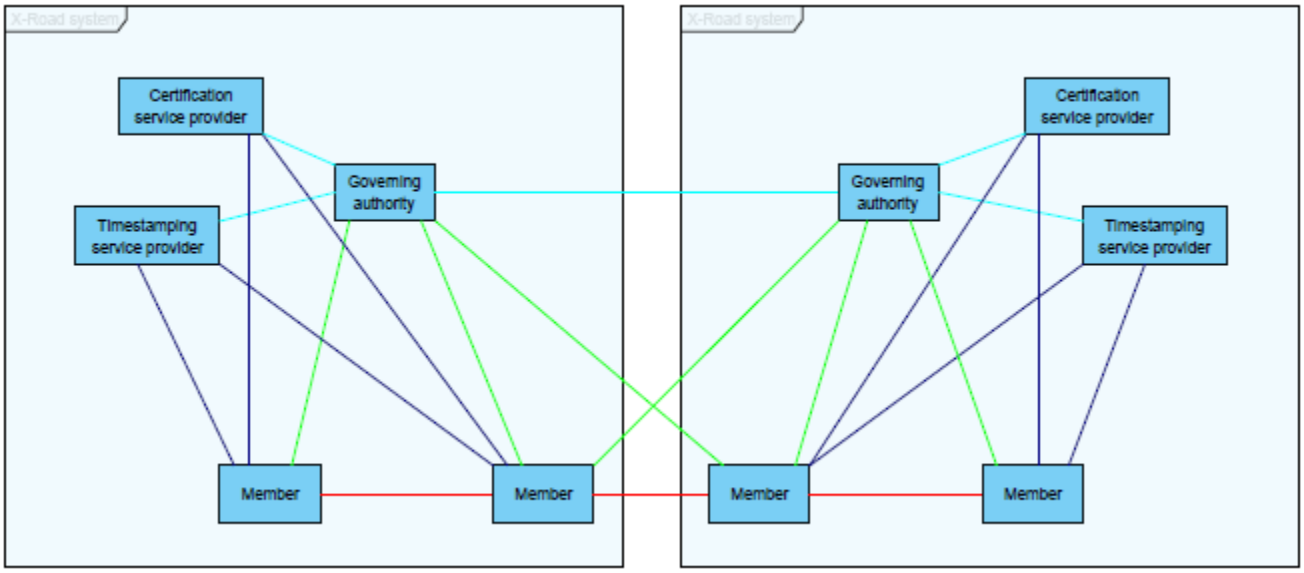

Fig. 3. Communication in federated X-Road system

federated system remain in control of the security policy of their native system.

- Establishing the federation relationship is carried out at the governing agencys level, the members do not have to make any additional arrangements.

To accommodate the aforementioned requirement a technical solution was proposed. Fig 3 represents the organization-level information flow in federated X-Road systems. The light blue lines indicate trust relationships, darker blue lines indicate the use of trust services, green lines indicate configuration distribution, and red lines for X-Road messages. The federation-capable X-Road system includes the following functional changes to the existing system

1) The configuration distributed by the X-Road governing authority is divided into internal and external parts [1].
2) The protocol used for configuration distribution is supplemented with the possibility to download only the external part of an X-Road systems configuration,

to allow the same protocol to be used for both internal and external configuration [1].

3) The existing system components- security server and central server is complemented with additional functionality for managing configuration [1].
4) Configuration proxies are developed to increase performance and reliability in slow network connections.

VI. Analysis

The system analysis was conducted on the following main models and components

- Conceptual model this model presents the participating entities in the configuration management and the relationship between the entities. The conceptual model includes the following configurations: A configuration provider maintains and distributes configuration. In the X-Road system, the configuration maintenance and distribution is performed by central server and configuration proxy. The system analysis was conducted on the following main models and components
- Conceptual model this model presents the participating entities in the configuration management and the relationship between the entities. The conceptual model includes the following configurations: A configuration provider maintains and distributes configuration. In the X-Road system, the configuration maintenance and distribution is performed by central server and configuration proxy.
- Business use case model - this model constitutes the federation relationship where the governing authorities of federation X-Road system agreed upon federation conditions and agreement.
- System component data model this model describes the data objects used and managed by the components for configuration management and distribution.
- System component use case models this model give a detailed description of the user-system interactions
- Component user interface specification this defines the user interface design and functionality among with roles and privileges.

References

[1] Analysis of Configuration Management in Federated X-Road Systems. https://digi.lib.ttu.ee/i/?2221

[2] Freudenthal, Margus, and Jan Willemson. "Challenges of Federating National Data Access Infrastructures." International Conference for Information Technology and Communications. Springer, Cham, 2017.

[3] HTTP: https://www.w3.org/Protocols/

[4] SOAP: https://www.w3schools.com/xml/xml_soap.asp

[5] WSDL: https://www.w3.org/TR/2001/NOTE-wsdl-20010315

[6] MIME: https://ccm.net/contents/120-mime-multipurpose-internet-mail-extensions

[7] X.509: https://msdn.microsoft.com/enus/library/windows/desktop/bb540819 (v=vs.85).aspx

[8] TLS: https://www.websecurity.symantec.com/security-topics/what-is-ssl -tls-https

[9] RFC: https://www.ietf.org/standards/rfcs/

[10] Federating X-Road installation https://www.ria.ee/en/introduction-of-xroad.html

[11] Willemson, Jan, and Arne Ansper. "A Secure and Scalable Infrastructure for Inter-Organizational Data Exchange and eGovernment Applications." Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, 2008.