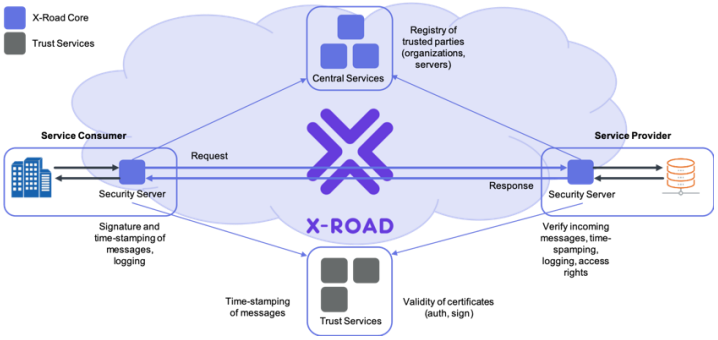
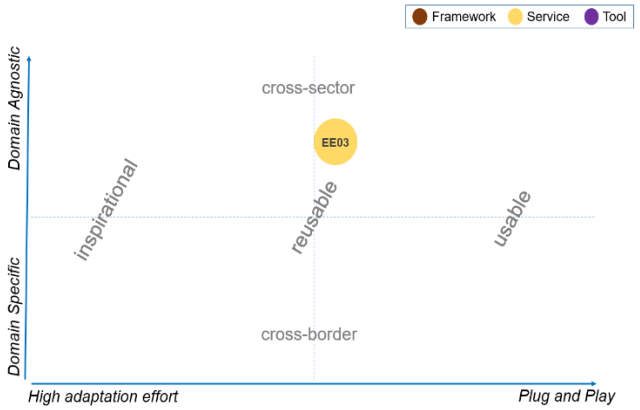
[EE03] X-Road

X-Road®			
Summary			
ID	EE03		
Initiative	Estonia, Finland, Iceland		
Short description	X-Road is a free and open-source data exchange layer solution that enables organisations to exchange information securely over the Internet. The basic idea of X-Road is that information systems do not exchange data directly with each other. Instead, information systems are connected through additional, standardised access points (Security Server) that implement the same technical specifications and therefore, can communicate with each other.		
Owner	Nordic Institute for Interoperability Solutions (NIIS)		
Contact	x-road.global	niis.org	info@niis.org
Type	Service		
Sub-Type	Infrastructure		
Context	Cross-sector, Cross-Border		
Base Registry type	All		
Operating model	X-Road is a centrally managed distributed data exchange layer between information systems that provides a standardised and secure way to produce and consume services. X-Road ensures confidentiality, integrity and interoperability between data exchange parties. **X-Road ecosystem** An X-Road ecosystem is a community of organisations 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 organisations 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 organisations. **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 organisation 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 organisation 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 organisation 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 organisations. 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 organisation can access its own data, whereas the X-Road operator can access all the members' data.
IPR	X-Road® is released under the MIT open source license and is available free of charge. X-Road® is a registered trademark of the Estonian Information System Authority (RIA).
Status	Operational
More details	
Aggregated business need	ABN – 8 Need for a technology solution enabling the data exchange
Functionalities	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. **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.

Design/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. **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. **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. **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. **Certification Authority (CA)** The certification authority (CA) issues certificates to Security Servers (authentication certificates) and X-Road member organisations (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.
Technologies	https://nordic-institute.github.io/X-Road-tech-radar/
Specifications	X-Road is data format agnostic, and supports transfer of any content type over HTTP using REST and SOAP based services.
Management	Nordic Institute for Interoperability Solutions (NIIS)
Governance	Nordic Institute for Interoperability Solutions (NIIS)

Sustainability	Nordic Institute for Interoperability Solutions (NIIS) is a non-profit association with the mission to ensure the development and strategic management of X-Road® and other cross-border components for e-government infrastructure. NIIS is both a network and cooperation platform and executioner of IT developments in members' common interests. The institute focuses on practical collaboration, sharing of experience and promoting innovation. The operating model of the institute is something unique in the world.
Documentation	Click Here
ADMS	Click Here
Current Users	Estonia, Finland, Iceland, The Faroe Islands, Germany, El Salvador, Colombia, Argentina, Japan, Vietnam, Azerbaidžan, Kyrgyzstan plus several other public and private implementations
EIRA	
View	Technical View - Application
Building Block	Application Service
Reusability	
Landscape	
Criteria