# D3.6 Feasibility Assessment of the Implementation of X-Road for Research Data

| | |
|---|---|
| Author(s) | Ahti Saar (UT/ETAIS), Ari Lukkarinen (CSC), Lauris Cikovskis (RTU), Ilja Livenson (UT/ETAIS) |
| Status | |
| Version | Final version |
| Date | 1.0 |

| **Document identifier:** | |
|---|---|
| Deliverable lead | ETAIS |
| Related work package | WP3 |
| Author(s) | Ahti Saar (UT/ETAIS), Ari Lukkarinen (CSC), Lauris Cikovskis (RTU), Ilja Livenson (UT/ETAIS) |
| Contributor(s) | Leah Riungu-Kalliosaari (CSC), Joni Virtanen (CSC), Juhani Nuorteva (CSC), Teemu Theqvist (CSC) |
| Due date | 31/08/2021 |
| Actual submission date | |
| Reviewed by | Abdulrahman Azab (UiO), Claudio Pica (SDU), Petteri Kivimäki (NIIS) |
| Approved by | |
| Dissemination level | Public |
| Website | https://www.eosc-nordic.eu/ |
| Call | H2020-INFRAEOSC-2018-3 |
| Project Number | 857652 |
| Start date of Project | 01/09/2019 |

| | |
|---|---|
| Duration | 36 months |
| License | Creative Commons CC-BY 4.0 |
| Keywords | Service(s), automation, framework(s) |


## Abstract:

This deliverable reports on the first iteration of feasibility assessment of using X-Road for cross-border research data exchange. It presents experience with setting up a data exchange service consuming data from Estonia, Finland and Latvia.

*Copyright notice:* This work is licensed under the Creative Commons CC-BY 4.0 licence. To view a copy of this licence, visit https://creativecommons.org/licenses/by/4.0.
*Disclaimer:* The content of the document herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.
While the information contained in the document is believed to be accurate, the author(s) or any other participant in the EOSC-Nordic Consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.
Neither the EOSC-Nordic Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.
Without derogating from the generality of the foregoing neither the EOSC-Nordic Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

## Table of Contents

**1** 6
**1.1** 6
**2** 7
**2.1** 7
**2.2** 7
**2.3** 8
2.3.1 8
2.3.2 9
2.3.3 10
**2.4** 11
**3** 12
**3.1** 12
3.1.1 13
3.1.2 13
3.1.3 13
3.1.4 14
**3.2** 14
**4** 15
**4.1** 15
**4.2** 15
**4.3** 16
4.3.1 17
4.3.2 19

**4.4** 22

**5** 23

**5.1** 23

**5.2** 24

**5.3** 24

**5.4** 25

**5.5** 25

5.5.1 25

**5.6** 27

5.6.1 28

**6** 30

**7** 31

**7.1** 31

7.1.1 31

7.1.2 32

7.1.3 34

# Table of Figures

Figure 1 Organizational model of X-Road from https://x-road.global/architecture. 9
Figure 2 X-Road architecture and main components. 10
Figure 3 Trust federation in X-Road. Multiple security servers per organization are typically used if an organization has memberships in several environments: production, testing or development. 11
Figure 4 GenMed story. Bold arrows correspond to communication over X-Road. 17
Figure 5 Dashboard of GenData application. 18
Figure 6 All requests for user data are logged and can be traced to the requestor and the declaration of intended usage. In this specific case GenComp from Estonia was accessing data from GenData in Finland over X-Road. 19
Figure 7 Dashboard of GenComp 20
Figure 8 Details view of a specific model in GenComp. 20
Figure 9 Summary report of an execution of analysis. Includes information about the specimen. 21
Figure 10 Summary information about the origin of the data of a specimen along with details about the Genetic Data Repository. 21
Figure 11 Summary report for running a model in GenComp deployed in Estonia on a person's data from registry in Finland. Decision for data source discovery is based on the prefix of the personal code, all communication is happening over X-Road. 22
Figure 12 Summary of pilot deployment for X-Road evaluation 23
Figure 13 X-Road subsystem exposing GenMed Genetic Data Repository in RTU. 29
Figure 14 Self-service of X-Road in Estonian deployment (X-Tee). The self-service is integrated with Estonina national catalogue of services (RIHA). 30
Figure 15 Overview of deployment of GenData with X-Road Security Server in RTU. 30
Figure 16 List of X-Road clients in UT X-Road server for EOSC-Nordic 32
Figure 17 Details of X-Road subsystem for GenData in UT. 33
Figure 18 List of clients for a subsystem, which exposes GenMed services in UT. 34
Figure 19 List of specific services exposed by an information system in UT through X-Road 34
Figure 20 Detail view of a specific service exposed via X-Road. Access rights as well as timeouts can be managed from this view. 35
Figure 21 Lookup of potential new clients of a service for authorization. Search is done across different environments trusted by the X-Road Security Server. 36

# 1 Executive Summary

The document describes the work performed when analysing feasibility of using X-Road-based solutions, adopted in Estonia and Finland, for exchanging research data. X-Road® is open source software and ecosystem solution that provides unified and secure data exchange between organisations. X-Road is developed by the Nordic Institute for Interoperability Solutions (NIIS), a nonprofit association established in 2017 by the governments of Estonia and Finland. Furthermore, the national X-Road environments in Estonia and Finland are federated, which allows for an easy technological way of establishing trustworthy communication between organizations participating in X-Road environments in Estonia and Finland.

To analyse the feasibility, we have partnered with a research group in University of Tartu[1], developing precision medicine solutions for clinical practice. The solution developed by them uses X-Road to receive requests from the clinical labs, access genomic data by analytical engine and to publish results to the Estonian Medical infosystem. For the proof of concept, we have taken the part of the solution responsible for providing genomic data and analysing it - and deployed that in 3 organizations across 3 countries: UT (Estonia), CSC (Finland) and RTU (Latvia), the latter joined Estonian X-Road development environment as part of the feasibility analysis. The resulting solution enables the scenario, where an analytical engine in one country is able to request on demand in a safe and efficient way the genomic data of a person from the registry in another country. We worked with development environments of X-Road and generated genomic data to avoid the extra burden of legal approvals, in other aspects the solution is equal to the production one.

In this document, we present the experience in setting up the proof of concept from organizational as well as technical sides and summarise initial findings. Overall we believe that adopting X-Road for real-time applications working with sensitive data has a good potential in R&D.

## 1.1 Document structure

The document is structured as follows:

1. In the **Introduction,** we provide background information on X-Road and explain its architecture.
2. In **Analysis of the X-Road adoption**, we present our findings about technical implications of adopting X-Road and analyse what applications would benefit from X-Road.
3. In **X-Road pilot deployment**, we describe the participants, application as well as overall deployment that was performed as part of the feasibility study in Task 3.2.3 of EOSC Nordic.
4. In the **Experience** chapter, we present our experience so far with the adoption.
5. In the **Next steps,** we provide our plans for the second phase of X-Road feasibility study.
6. Finally, **Appendix A** provides an example of the actual configuration of the X-Road Security Server in the UT environment along with explanations of the typical steps.

[1] https://sisu.ut.ee/genmed/en?lang=en

# 2 Introduction

## 2.1 X-Road history

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 development began in the late 90s and a pilot version was presented in 2000. From 2001, Estonia has shared its experiences with several countries including Finland, Iceland and others[2]. In 2013 the Prime Ministers of Estonia and Finland signed the Memorandum of Understanding to further develop X-Road. This is considered to be the world's first digitally signed international agreement. Since then, cooperation between these two countries has increased drastically.

Another important outcome of the collaboration between Information System Authority of Estonia (RIA)[3] and Population Register Centre of Finland (VRK)[4] was publishing the source code of X-Road core as open source under the MIT free software licence. The source code was published in two parts in 2015-2016 and it was made publicly available to anyone. Since then, dozens of countries around the world have implemented X-Road as their national data exchange layer solution. The cooperation between Estonia and Finland has had a global impact.

In 2017, Estonia and Finland decided to deepen the cooperation by forming a joint organisation to administer the development of X-Road. The formation and cooperation agreement of the Nordic Institute for Interoperability Solutions (NIIS)[5] was signed by ministers of the two countries. From June 2018, NIIS took over the responsibility of the joint X-Road development and the management of the source code of X-Road core. In 2021 Iceland joined NIIS as the third member. NIIS is a member of GAIA X AISBL.

## 2.2 Current status

Using national registers as a part of everyday life is quite common. From the end-user perspective, it is invisible which kind of requests are made to fulfill the requestor's need. For example, when buying an insurance policy for a car, the insurance company will make a request to the transportation registry to check whether this person has the right to buy an insurance policy for a particular car or not. Another example is that when a person is e-voting, then the system will make a request to the e-population register to find out whether a person is old enough to vote and to collect information about the person's residential address for displaying candidates based on this location. All these requests must be made securely and efficiently, so X-Road technology fulfills these needs.

---

[2] https://x-road.global/xroad-world-map
[3] https://www.ria.ee/en.html
[4] https://dvv.fi/en/individuals
[5] https://www.niis.org/

As of August 10th, there are 633 organizations in Estonia, which are using the X-Road data exchange layer and there are organizations offering 2961 services in total. Approximately 52 000 organizations are indirectly using services via X-Road technology[6].

In Finland, there are 173 organizations offering 394 services[7].

The data services available over X-Road systems in Estonia and Finland are mostly government registries, e.g. building registries, medical records, ship and vehicle registries, etc. “Why” data owner should provide access to the data is generally outside the scope of X-Road. It can be mandate by law or could be based on person’s permissions (e.g. accessing of medical records by family doctor).

Overall, X-Road provides a very sustainable infrastructure for sharing data among different entities, including cross-border scenarios. This property was one of the main motivations to evaluate X-Road’s fitness for a more academic setup.

## 2.3 X-Road architecture

X-Road / NIIS maintains an excellent documentation introducing the ecosystem and architecture of an X-Road deployment. We encourage readers to go through the documentation at https://x-road.global/. Below we include a small subset of the information to simplify understanding of the current document.

### 2.3.1 Organizational model

X-Road defines several roles[8] that are needed for deployment of an X-Road environment:

- **Operator** - runs central services and enforces rules of participation;
- **Trust service providers** - Certification Authorities and Time Stamping Authorities providing cryptographic services for establishing digital trust in a system.
- **Members** - organisations who provide and consume web services and APIs. The role that most participants in X-Road have.

[6] https://www.x-tee.ee/factsheets/EE/#eng
[7] https://liityntakatalogi.suomi.fi/en_GB/
[8] https://x-road.global/x-road-organizational-model

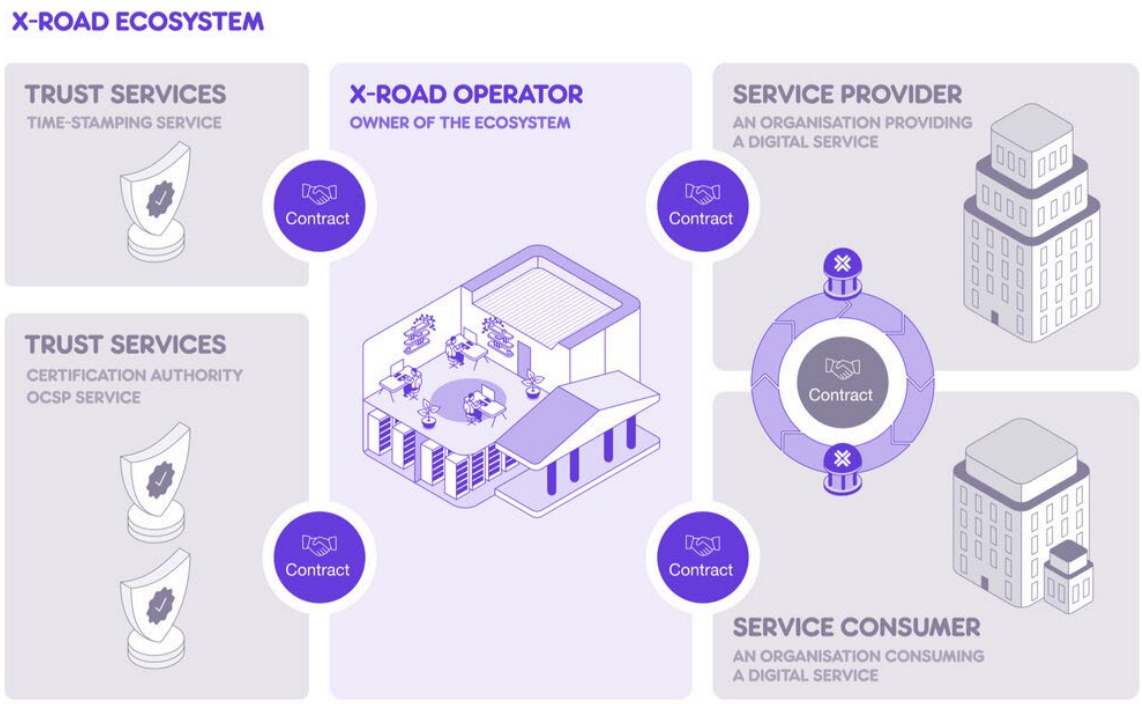



*Figure 1 Organizational model of X-Road from https://x-road.global/architecture.*

### 2.3.2 Components

X-Road consists of several components which interact with each other in a loosely coupled fashion. The main ones from our piloting perspective are:

- **Central services**, which provide a registry of services and members available in the environment (i.e., validated and following the rules of participation) as well as a list of trusted Certification Authorities.
- **Security Server**, which serves as a gateway into the X-Road environment from the member view. Security Server can be operated by the member or can be provided as a service by a trusted third party. It connects services as well as consumers of services from a specific organization with the rest of the information systems in the environment. A Security Server is deployed for each of the organizations and is registered in the central services.

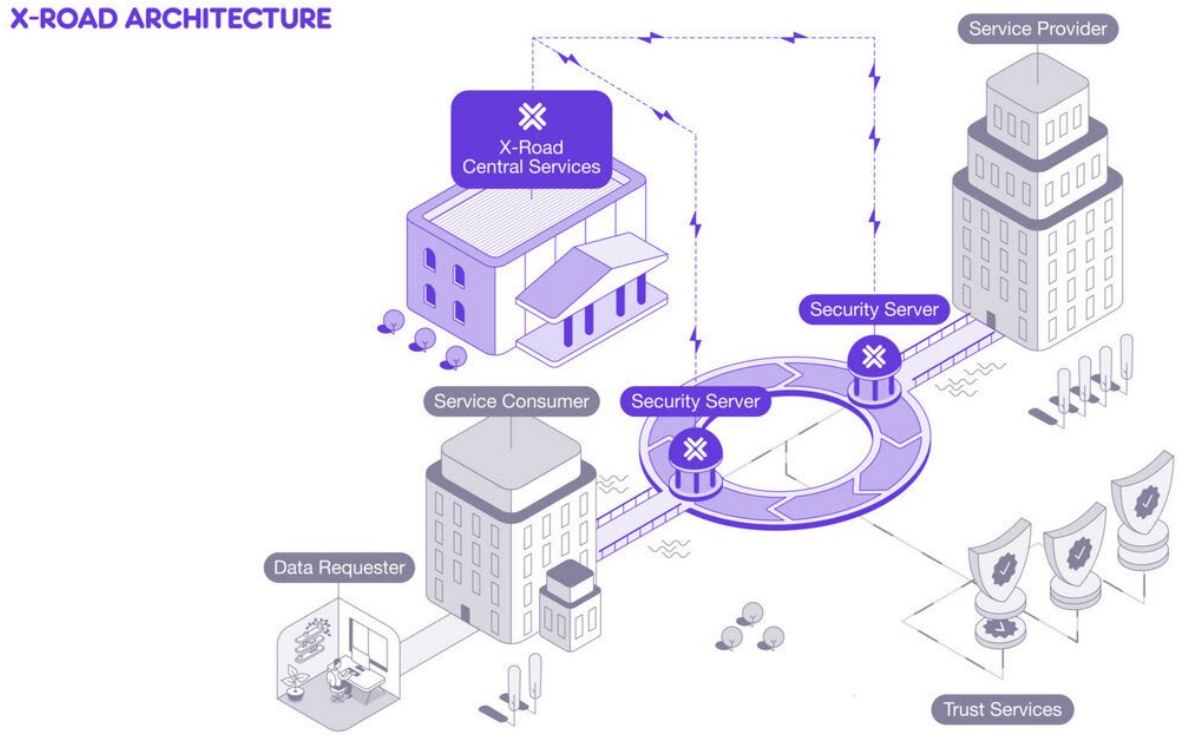



*Figure 2 X-Road architecture and main components*[9].

In case a service provided by a service provider is able to provide a REST API, it can be published as-is to X-Road. This is the most likely method to connect new services to X-Road. X-Road REST API supports OpenAPI 3 service descriptions as well as manual endpoint creation. Also, it's possible to define access to REST APIs on two levels: REST API level and endpoint level. When access rights are defined on the API level, they apply to all the endpoints of the API. Instead, defining access rights on the endpoint level enables more fine-grained access rights management.

### 2.3.3 Federation

Each deployment of X-Road is controlled by specific rules and has a separate operator of central services. In case such environments should support interactions among each other, it is possible to use federation of X-Road. X-Road federation makes it possible to exchange trust, registry data and allows clients from one environment to talk to services in another.

In practice that means among other things alignment of legal basis for cross-border data and metadata exchange. In particular, this has been done between Estonia and Finland and was

[9] https://x-road.global/architecture

adopted by the first production service - exchange of data between Estonian and Finnish business registries[10] in March 2019.

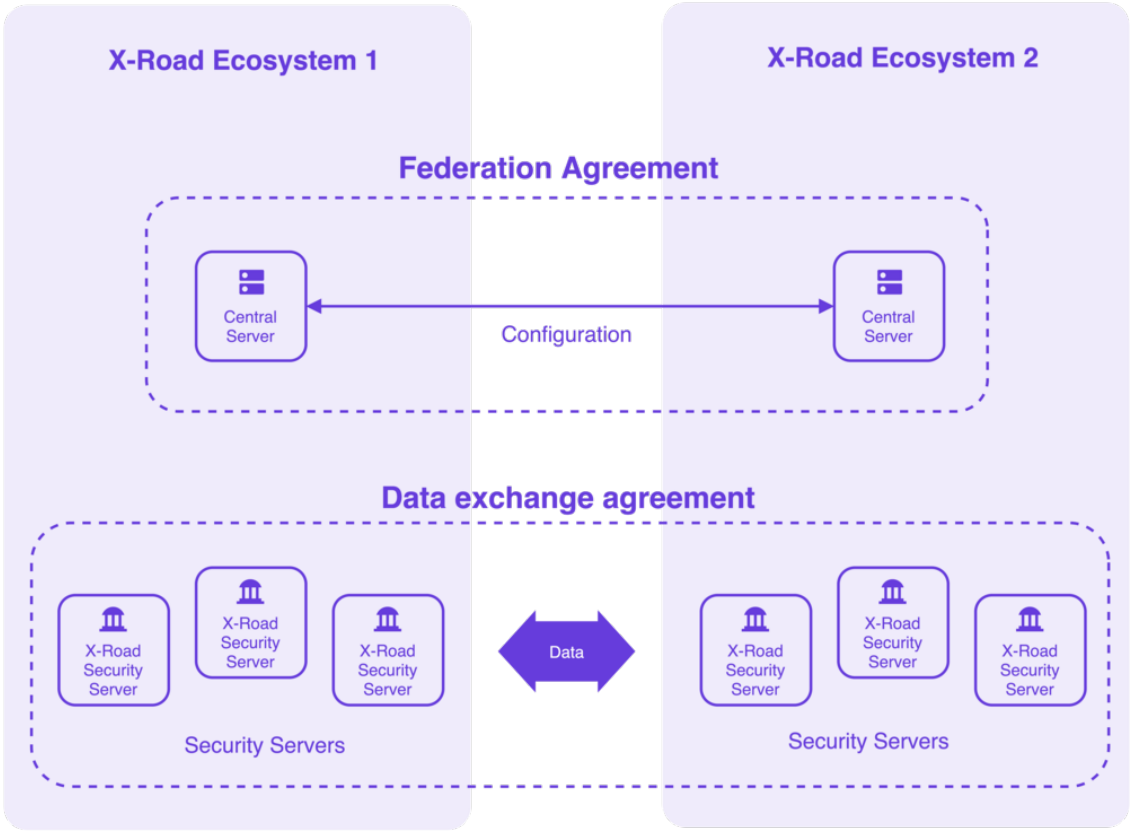



*Figure 3 Trust federation in X-Road[11]. Multiple security servers per organization are typically used if an organization has memberships in several environments: production, testing or development.*

Federation is very important as it allows to scale deployments by establishing environments in more naturally governed setups (e.g. within an organization or within a country) and agree on specifics of interactions across them. Federation is widely used also in research environments partially also to work around the governance issues.

## 2.4 National catalogues and example deployments

Estonia has its own state's information system called RIHA[12]. It has two main goals: to list all available information systems in Estonia, users of these information systems and data which is available and processed; the second goal is to manage information systems: add new ones, edit or remove existing ones. These systems are equivalent to the X-Road clients and subsystems.

[10] https://x-road.global/case-study-the-business-registers-of-estonia-and-finland . Legal agreements are available at https://www.ria.ee/sites/default/files/content-editors/XTEE/trustfederation_xtee_palveluvayla.zip
[11] https://x-road.global/trust-federation
[12] https://www.ria.ee/en/state-information-system/administration-system-riha.html

In Finland, information about the services connected to Finnish X-Road, known as Suomi.fi Data Exchange Layer, is available publicly[13] in the Suomi.fi API Catalogue. Currently, there are 27 service providers, 173 organizations, and 395 public subsystems. The Finnish X-Road is being developed by the Digital and Population Data Services Agency[14].

The table below shows some examples of use-cases where X-Road is used today, beyond the national use-cases mentioned above[15].

| **Context** | **Country** | **Need** |
|---|---|---|
| Medical video consultation and digital prescriptions | Germany | Secure data storage and exchange supporting an e-prescription portal |
| Information exchange between national business registers, tax boards and population registers | Estonia, Finland | Connecting the two governmental agencies via X-Road |
| Information exchange of customers' data across sub-companies | Japan | Efficient information exchange of clients' data in the energy sector |
| Implementation of national data exchange layer | El Salvador | Cross-agency modernization of public administration practices |
| Digitising services for citizens, industries and the public sector | The Faroe Islands | Implementation of X-Road at a national level |

# 3 Analysis of X-Road adoption implications

## 3.1 Technological implications of X-Road

X-Road refers to technology, i.e. open-source solutions, and actual deployments use their own names[16] with their rules of participation. Below we analyse implications of adopting X-Road for cross-border research data exchange.

[13] https://liityntakatalogi.suomi.fi/en_GB/
[14] https://dvv.fi/en/digital-and-population-data-services-agency
[15] https://x-road.global/piloting-digital-prescriptions-in-germany-through-secure-data-exchange
[16] For example, X-tee in Estonia, Suomi.fi Data Exchange Layer in Finland, Tenoli in El Salvador, CamDX in Cambodia.

### 3.1.1 Performance

X-Road data exchange works by sending digitally signed messages through a secure channel established by security gateways between the information systems of X-Road participants. As such, X-Road brings both the overhead for data size as well as processing of the data. In production environment in Estonia, messages can be signed only by Hardware Security Modules[17], which typically are expensive if higher performance is required.

As such, X-Road is rather used for exchanging smaller amounts of data and not for e.g. streaming or mass data replication. For smaller payloads the overhead is negligible.

### 3.1.2 Security

X-Road is built with security as one of the main goals. As such, it includes a lot of features that allow to assure that messages are queried and delivered by and to exactly the authorized parties. X-Road deployments mainly rely on eIDAS-compliant Trust services for ease of legal alignment. Technical, however, mandatory is to support X.509 certificates with RFC 6960- compliant OCSP service and RFC 3161-compliant time-stamping service. Extensions of the X-Road protocol[18] allow to reference identities of the users within a query, whose data is transferred, to allow users to audit who and for what purpose used their data.

X-Road software is professionally developed and is used in highly sensitive deployments. Current security activities in X-Road development include:

- regular security assessments conducted by a third party, including architecture review, threat modelling, penetration testing;
- source code reviews;
- threat modelling;
- static source code analysis;
- dependency checks;
- public bug bounty program[19].

Data transfers over X-Road are encrypted in transit on a transport layer, i.e. between the two Security Servers.. All endpoints are explicitly authorized, i.e. service owners must allow access to certain services by other organizations explicitly.

### 3.1.3 Trust

Under trust we understand processes that allow different stakeholders of the system to establish and maintain trust relationships with each other.

---

[17] https://en.wikipedia.org/wiki/Hardware_security_module
[18] https://github.com/e-gov/AJ (mostly in Estonian)
[19] https://app.intigriti.com/programs/niis/x-road/detail

On the technological level, trust is mostly delegated - to operators of central services and trusted service providers. Otherwise, each member - provider or consumer - is responsible for their own system.

In addition, operations in production deployments are governed by rules - mandates and laws in case of Estonian and Finnish deployments - which provide an additional level of trust.

### 3.1.4 Ease of adoption

Integration of services with X-Road is relatively straightforward - all integration happens via the X-Road Security Servers, which support WSDL and OpenAPI interfaces, so services that are being integrated are expected to support those interfaces. Also, publishing REST APIs without an OpenAPI description is supported.

Integrating existing services with X-Road is relatively straightforward. There are examples, training materials[20], community support as well as dedicated support units for specific X-Road environments that have SLAs for support.

Overall we consider that technological complication of integration of services with X-Road is low to medium, if a separate connector needs to be developed - mainly for non-REST APIs. In practice, this connector should have access to the service and SOAP API with well-defined endpoints.

Use of well documented APIs enables wider use of functionally more or less similar but internally different services. This is because X-Road by itself doesn't set any requirements to services attached to it - how endpoints are named, how HTTP verbs are used, API versioning, error messages, etc. So, in principle it would be possible that more or less identical services would have different APIs on X-Road. This obviously would complicate the overall integration task as there is no guarantee of compatibility on the semantic level.

On the production deployment side, the requirement of a high level of assurance when joining the X-Road environment can mean additional effort if the organization is larger and more effort is needed to establish representation rights.

## 3.2 Why use X-Road in a research context?

X-Road is mostly used for connecting data registries that contain sensitive data with processors of the data. Furthermore, typical consumers of the data are used in online services, i.e. expect to get quick access to required data based on pre-existing agreements. Such use cases are becoming increasingly more interesting in R&D context as well, in particular granular access to sensitive data repositories.

[20] https://x-road.global/resources

X-Road enables reliable transfer of sensitive data. However, sometimes security provided by X-Road is not enough or there are other reasons why the data cannot leave the target service. In such cases, giving a slightly modified access to data or by moving data processing tasks to the service provider's infrastructure could be considered. An example of the first case would be e.g. automatic anonymization of structured data. This anonymization could be done by the service itself. Access to anonymized data would only need a specific REST API endpoint.

X-Road deployments are also typically well-funded and have a clear sustainability model. This allows solutions to be built on top of X-Road with a low risk related to the sustainability of the underlying data exchange layer.

Existing X-Road deployments are not greenfield deployments - they contain a number of existing organizations from the public sector that own and expose registry data that is of interest also for research purposes. In practice, it means that consuming data over X-Road allows to reuse two aspects of data acquisition:

- The governance aspect of validating endpoints of data interactions and understanding who is responsible for allowing data to be exchanged.
- The technical aspect of connecting to new data sources - standardized via X-Road security gateways.

# 4 X-Road pilot deployment overview

The goal of the feasibility study was to understand how X-Road can improve the situation with exchange and processing of research data in existing organizations.

Below present the components of the practical evaluation.

## 4.1 Participants in the pilot deployment

While X-Road is widely used for communication among organizations in the same country, our goal was to understand its actual use in a **cross-border** scenario. For that, we have chosen 3 organizations from 3 countries:

- CSC in Finland;
- University of Tartu in Estonia;
- Riga Technical University in Latvia.

These organizations are active in both research and the EOSC landscape.

## 4.2 Selecting X-Road environment for the pilot

X-Road deployments are called environments. The environment comes with a specific set of rules of participation as well as an ecosystem of services.

Estonia and Finland have their national X-Road deployments in place – the Estonian X-tee and the Finnish Suomi.fi Data Exchange Layer. Also, there is a federation established between the two environments, so we decided to use those: X-tee for University of Tartu and Suomi.fi Data Exchange Layer for CSC. As Latvia does not have a national deployment, we investigated if Latvian organization could join the Estonian or Finnish environment. Fortunately, it was legally possible in both cases, but the Estonian one was easier to connect to due to the presence of the E-Residency service, which allowed a Latvian representative to get electronic identity and perform actions online[21]. So RTU from Latvia ended becoming a member of the Estonian X-tee and could communicate with UT in Estonia over the same environment and with CSC in Finland using federation.

It should be noted that we have also considered deploying our own X-Road environment along with simplified rules of participation (e.g. without strong validation of representation rights), however the effort for maintaining would go beyond the size of the task.

## 4.3 Pilot application

To validate X-Road, we have selected an actual application that has components serving as data providers as well as data consumers. The application is being developed in a project codenamed GenMed[22], within a consortium including several departments of University of Tartu - the Computer Science department, the Centre of Personalised medicine and health informatics, Institute of Genomics – as well as National Institute for Health Development, Estonian Health Insurance Fund and IT department of Ministry of Social Affairs. The project is not yet complete, but the software solution was already mature enough to satisfy the needs of our feasibility assessment in EOSC-Nordic. We are very thankful to the lead developer Martti Tamm for providing assistance and custom development of GenMed to fit EOSC Nordic use cases.

Quoting the project's info page, the aim of the GenMed project is to build the necessary IT infrastructure in Estonia to apply personalised medicine principles in clinical practice so that personalised medicine could benefit all people in Estonia. In the course of the project, solutions for pharmacogenetics and polygenic risk scores are introduced as part of the national e-health system. This results in suggestions in prescriptions about drug dosage, as well as indicating the inherited risk of diabetes and heart disease based on the patient's DNA.

From the deployment perspective, produced software helps to support the process, where a patient comes to a doctor, who would then request a test for that patient (identified by ID in eIDAS-compliant format[23]) from a certified lab. The lab would then submit the test to the GenComp's environment, which contains a repository of certified models for analysis as well as processing facility. The processing facility then loads the model corresponding to the test requested as well as requests required genomic snippets from the corresponding Generic Data repositories. For the

[21] The process is described in more detail in 5.6 X-Road experience: RTU/Latvia.
[22] https://sisu.ut.ee/genmed/en?lang=en
[23] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile , Unique Identifier attribute

pilot, we made the assumption that genomic data of the people would reside in the country, which has emitted their ID codes, and so the GenComp was extended to route the request according to the country code found in the person's ID code.

After the processing, the results are uploaded to the National Health Information System where it can be accessed by doctors and people themselves.

The whole application includes a large number of stakeholders and is deployed in a well regulated environment. For the purposes of our task, we have concentrated on the X-Road interaction between the GenMed components: Processing engine codename GenComp and Genetic Data Repository codenamed GenData.

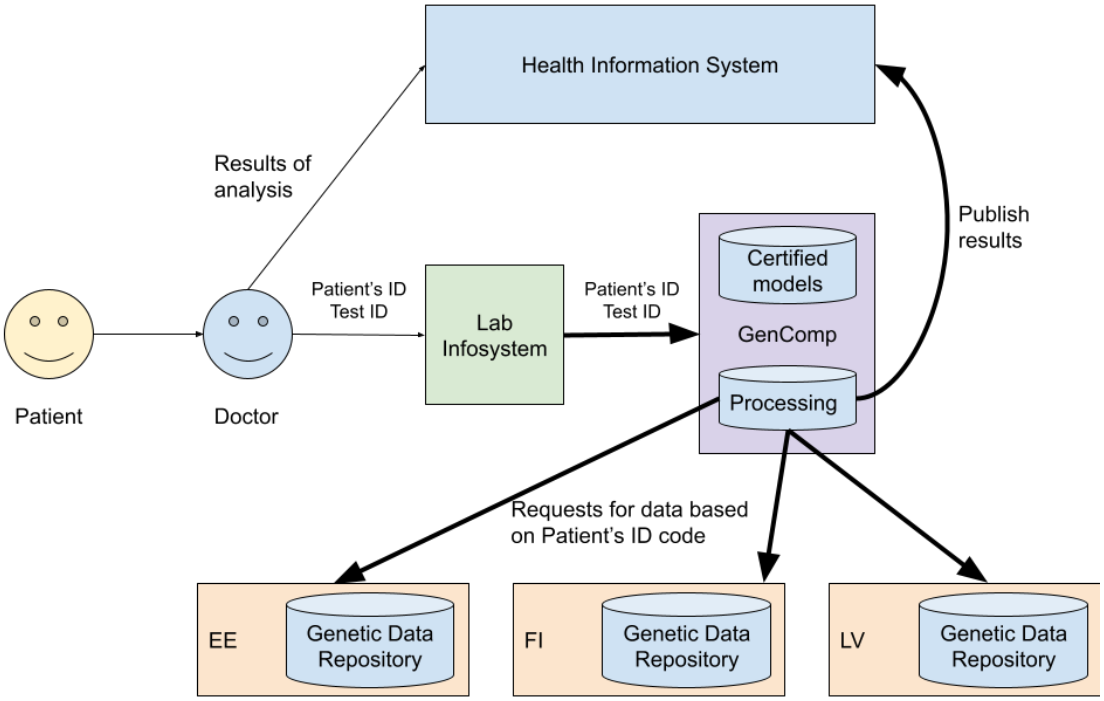



*Figure 4 GenMed story. Bold arrows correspond to communication over X-Road.*

Both components include a lightweight user interface for monitoring of the status, showcased below.

### 4.3.1 GenData

GenData is a repository exposing several functions for secure access to snippets of genetic data over X-Road. It allows users to submit data from different sources, mark it for use for target audiences, manage encryption keys as well as retrieve the requested snippets of the data.

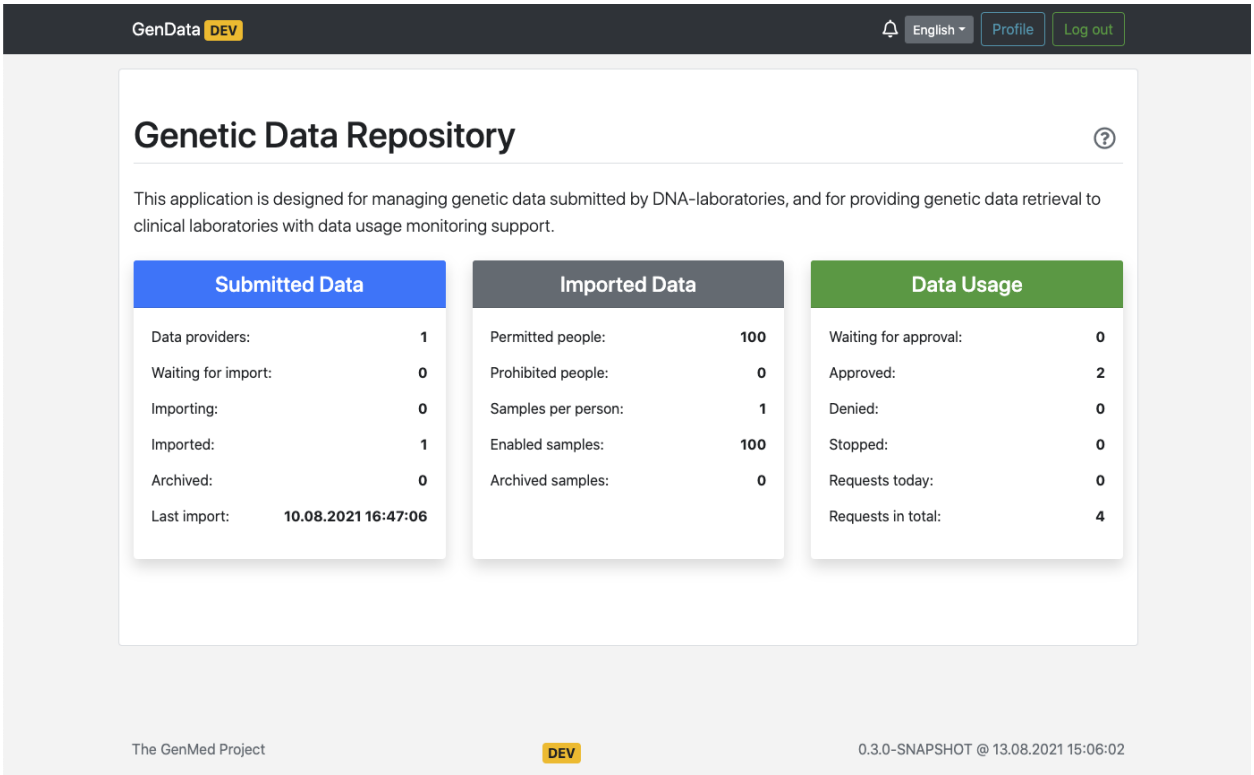



*Figure 5 Dashboard of GenData application.*

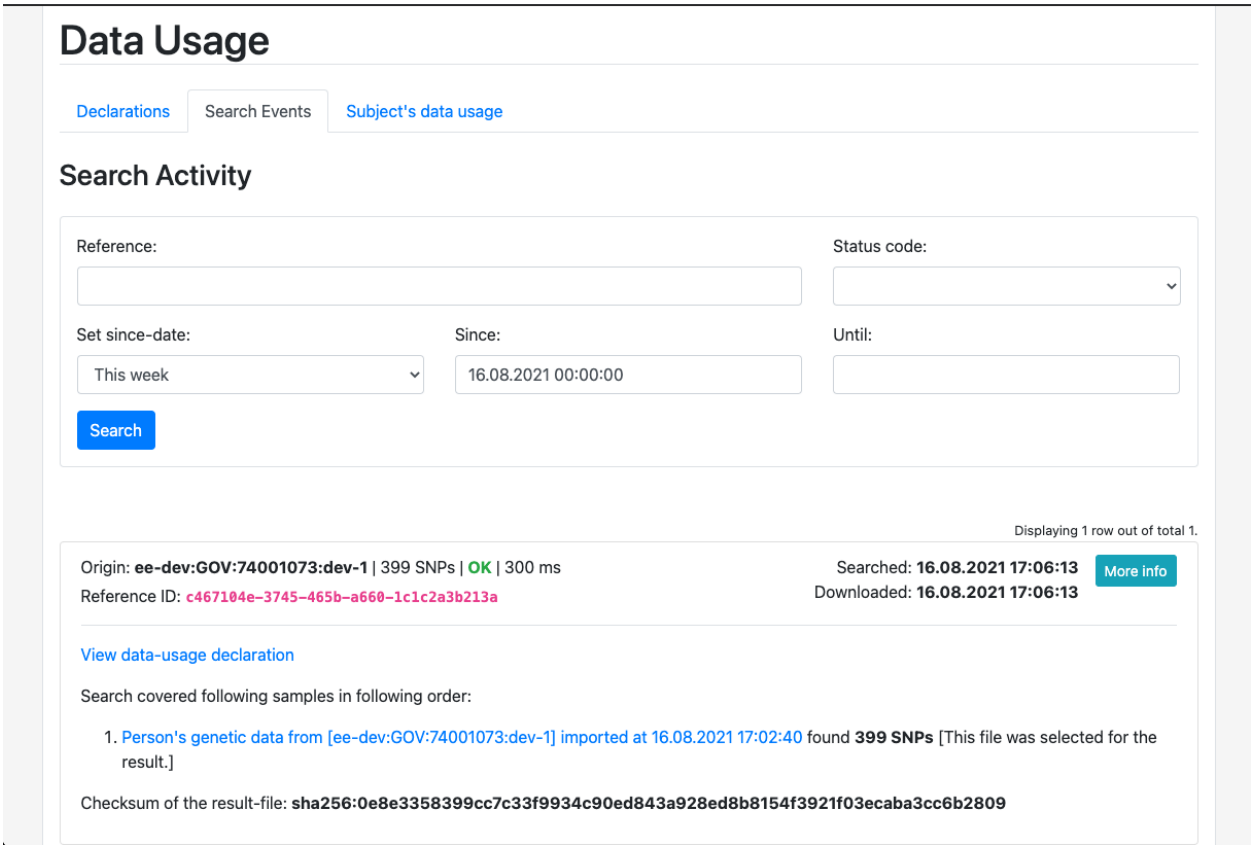



*Figure 6 All requests for user data are logged and can be traced to the requestor and the declaration of intended usage. In this specific case GenComp from Estonia was accessing data from GenData in Finland over X-Road.*

### 4.3.2 GenComp

GenComp is an application, which manages models that can be used for running computations on genetic data. Execution of a specific model supports downloading of data from the Genetic Data Repository corresponding to the personal code through X-Road protocol.

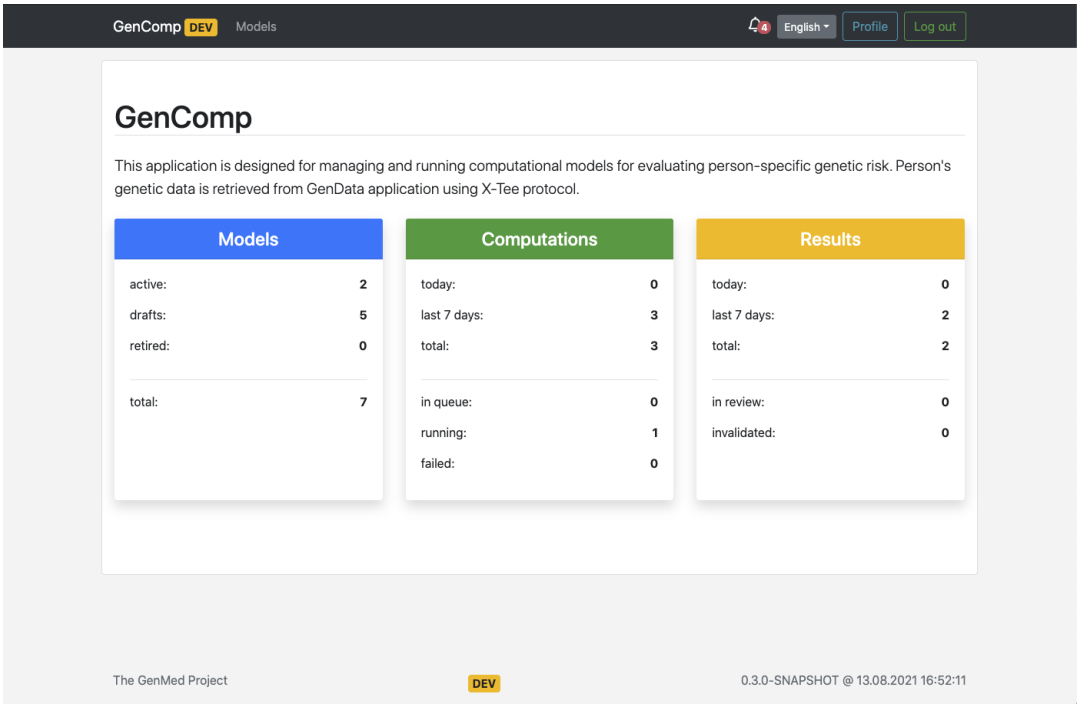



*Figure 7 Dashboard of GenComp*

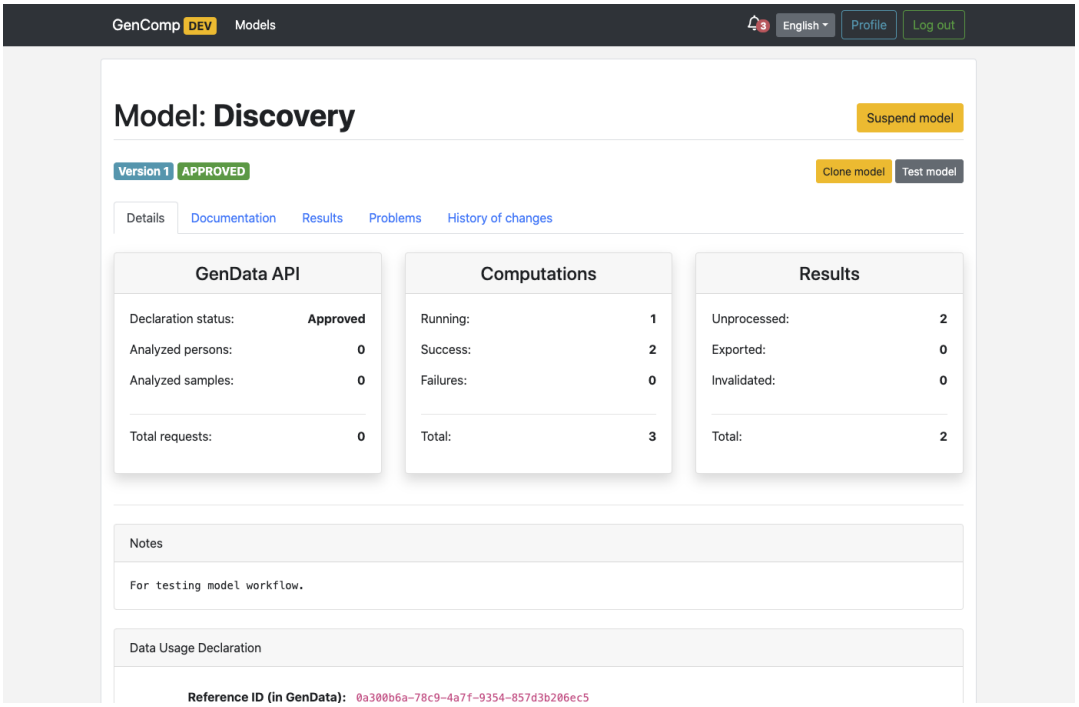



*Figure 8 Details view of a specific model in GenComp.*

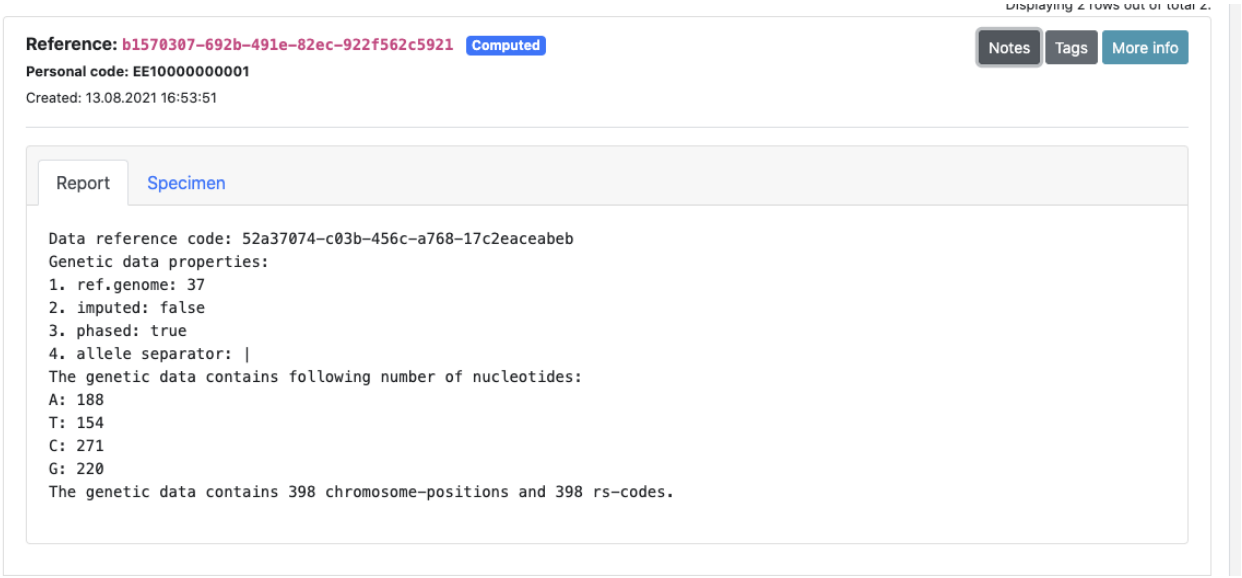



*Figure 9 Summary report of an execution of analysis. Includes information about the specimen.*

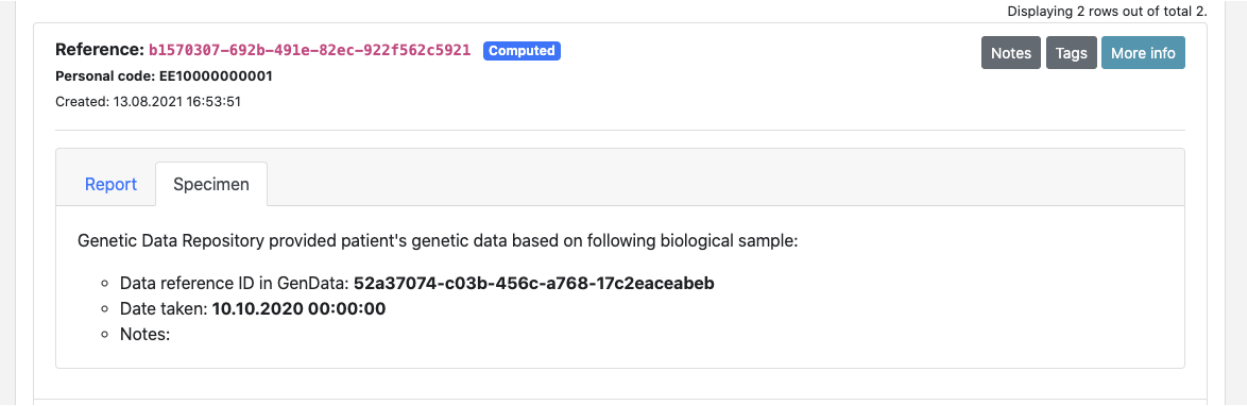



*Figure 10 Summary information about the origin of the data of a specimen along with details about the Genetic Data Repository.*

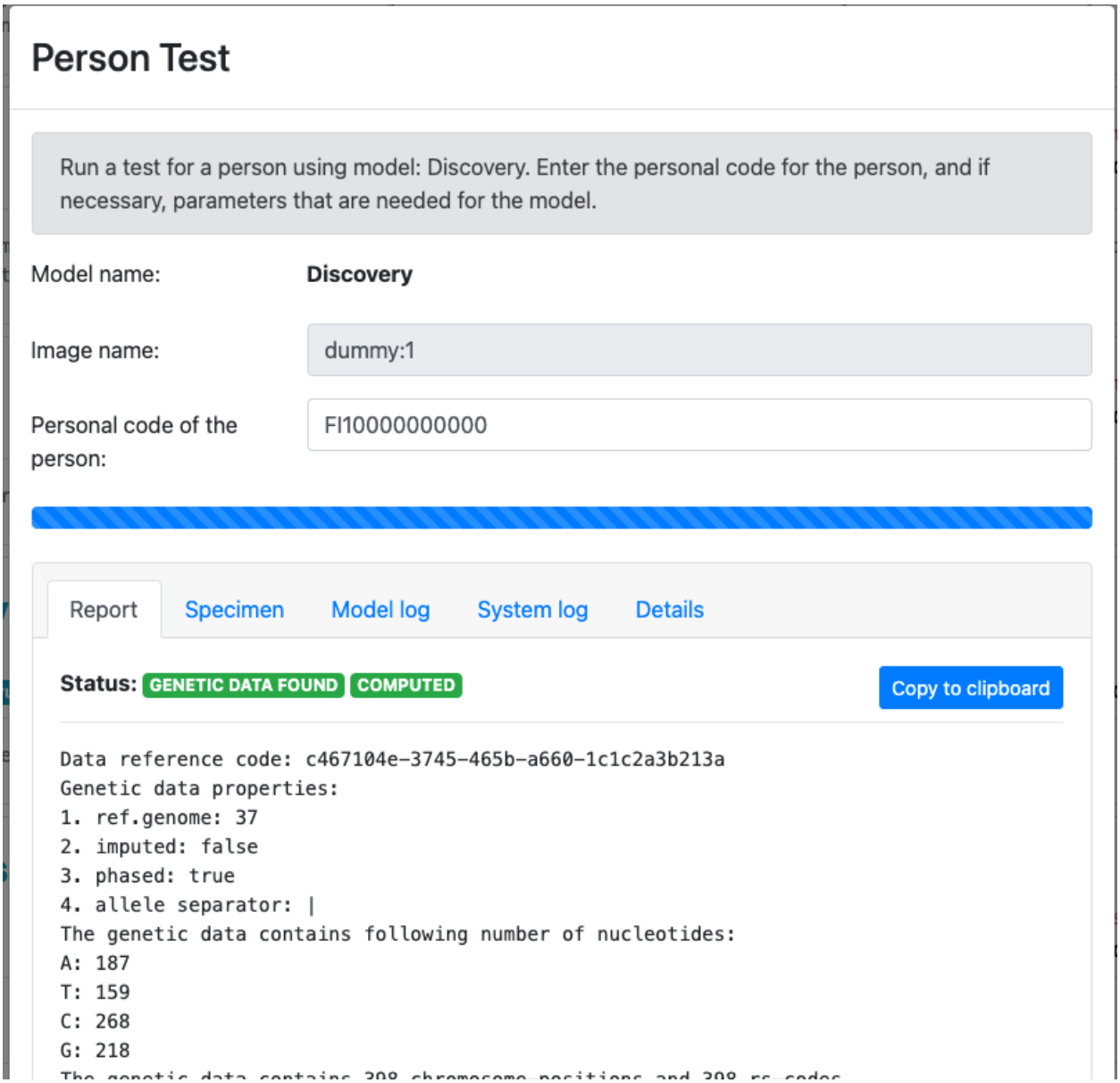



*Figure 11 Summary report for running a model in GenComp deployed in Estonia on a person's data from registry in Finland. Decision for data source discovery is based on the prefix of the personal code, all communication is happening over X-Road.*

## 4.4 Deployment summary

Our pilot deployment of GenMed was done with the following main characteristics:

1. There are 3 data providers deployed in 3 different organizations in 3 countries.
2. UT and RTU are connected to the Estonian X-Road environment, whereas CSC is connected to the Finnish one. Federation between environments has been enabled in all 3 organizations.

3. UT additionally runs a data consumer – a GenMed module, that requests data from the data providers and runs the analysis before uploading the results to the target medical infosystem (the upload step is outside the pilot scenario).
4. UT, RTU and CSC have authorized Data consumer subsystems for accessing the data.
5. For demonstration purposes, data providers also allow injection of mock data from data Consumer via X-Road.

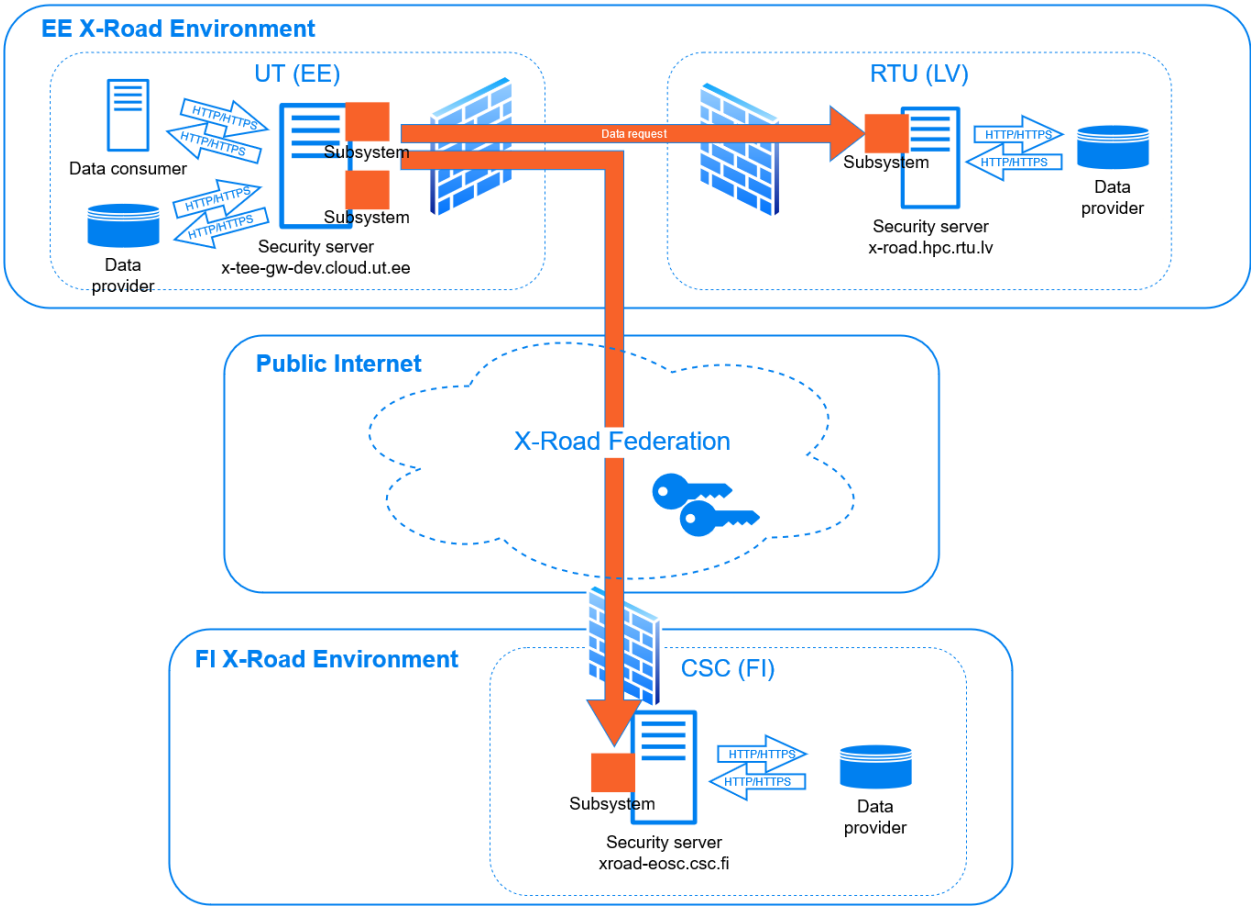



*Figure 12 Summary of pilot deployment for X-Road evaluation*

# 5 Experience

## 5.1 Strong validation of stakeholders

Strong validation of organizations simplifies decision making for establishing cross-border communication. While strong validation means potential extra work in initial setup – as was demonstrated by case with RTU (Latvia) joining Estonian X-Road environment – having a network where endpoints have high level of assurance on the organizational level makes it easier to

establish data exchange with sensitive data, which requires legally binding agreements for exchange.

A similar problem is being solved by the EOSC Provider portal and on-boarding team in EOSC Future, although no strict validation of representation rights is done. This has led to issues where representation rights of an organizational entry are not fully validated and can pose potential issues in the long term.

It should be noted that using X-Road for distribution of open access data is most probably not efficient as the overhead of validation would not serve any further purpose, unless non-repudiation and integrity of such data would be required.

## 5.2 Alignment with EOSC Interoperability Framework

X-Road is an interoperability framework for data exchange in the public sector. It follows European Interoperability Framework (EIF) tightly and concrete deployments of X-Road, in particular in Estonia and Finland, fulfill majority of the EIF guidelines on legal, organizational, semantic and technical level (though the latter is mostly limited to the aspect of data exchange and not structure of the exchanged data).

As EOSC Interoperability Framework is among others based on EIF, adopting X-Road for service federation improves adherence to the EOSC IF guidelines.

## 5.3 Selecting an application for the proof of concept

In order to validate usage of X-Road for scientific use cases, we wanted to select an application that would benefit from distributed data sources as well as do non-trivial calculations.

Those services that are not at the moment connected to X-Road would require some modification to be done on the service side. In case a service provides a REST API, accessing service would in principle be easy. However, it is likely that without modifications, the service would not be able to utilize the X-Road infrastructure. Therefore, as a starting point we decided to try to use existing implementations as much as possible.

Unfortunately, there was a limited amount of information about the connected applications available in catalogs for the X-Road development environment and testing and production environments would require additional justification for requesting access, as they contain actual data. Eventually, we partnered with a research group from University of Tartu, which is developing applications for personalized medicine, and used their GenMed application as a pilot application.

## 5.4 X-Road experience: UT/Estonia

University of Tartu (UT) is a public university in Estonia. It has been a member of X-Road for a while, mostly for integrating with services of the Ministry of Science and Education (student admission data and research project metadata management). Internally UT also has a clear system of getting confirmations for requesting access and getting new X-Road clients in place. For higher flexibility with experimentation within EOSC Nordic, a new X-Road Security Server in the EE development environment was deployed.

For UT, deployment of the X-Road development environment was handled by the HPC team participating in the EOSC-Nordic project and the GenMed application is maintained by the corresponding project team. Topological deployment is identical to RTU's, described in 5.6, so we skip it here for brevity.

## 5.5 X-Road experience: CSC/Finland

CSC - IT Center for Science is a non-profit state enterprise with special tasks. As part of the national research system, it develops, integrates and provides high-quality information technology services and ensures that Finland remains at the forefront of development. CSC is owned by the Finnish state (70% shareholding) and higher education institutions (30% shareholding).

CSC has been active in X-Road service since 2014, when the X-Road version 5 test environment was maintained by CSC. Later, X-Road was included into KAPA (national service architecture implementation program)[24] and the *Digital and Population Data Service Agency*[25] started operating the service. CSC is still actively participating in service development in the Finnish X-Road environment.

CSC has already been registered in X-Road, but deployed a separate instance of X-Road Security Server to have more freedom of experimenting.

### 5.5.1 Deploying X-Road software

Finland and Estonia use the same packages, but different default configuration, so the installation process is a bit different from the Estonian process. GenMed software was deployed in a separate virtual machine using docker-compose. For the X-Road, the process is summarized below. Packages are installed from the Finnish mirror of X-Road repository.

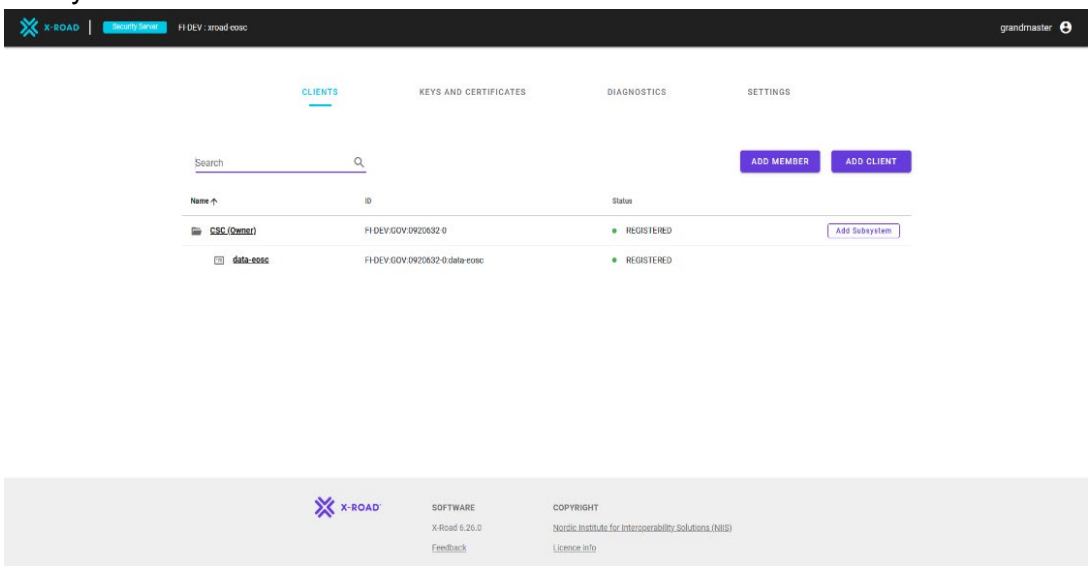
a. To install X-Road services, the following installation commands were used:
```
sudo apt-add-repository -y "deb http://www.nic.funet.fi/pub/csc/x-road/client/ubuntu-test-current/packages focal-current main"
```

[24] https://julkaisut.valtioneuvosto.fi/handle/10024/160710
[25] https://dvv.fi/en/

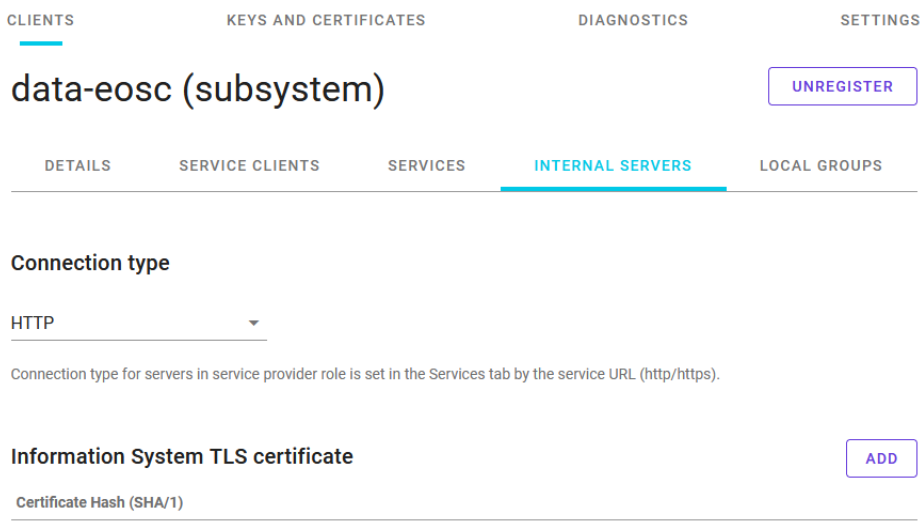
```
curl http://www.nic.funet.fi/pub/csc/x-road/client/ubuntu-test-
current/niis.public.asc| sudo apt-key add -
adduser grandmaster
locale-gen fi_FI.UTF-8
update-locale fi_FI.UTF-8
apt-get update
apt-get install xroad-securityserver-fi
```

b. The X-Road configuration guide that was used:
   i. X-Road installation guide: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/5931237e03f6d100018db62b
   ii. X-Road configuration guide: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/59145e7b14bbb10001966f72

c. X-Road graphical interface configuration
   i. Subsystem information




   ii. Connection type between data-eosc.csc.fi (backend, GenMed application) and xroad-eosc.csc.fi (Security Server)




iii. The Security Server authentication and signing keys are valid until 07.10.2024. After this they must be renewed if the federation connection is still needed.

## 5.6 X-Road experience: RTU/Latvia

Unlike Estonia and Finland, Latvia is not part of X-Road collaboration and hasn't implemented X-Road at the national level. Nevertheless, Estonia information systems Authority (RIA) does not limit participation of organisations registered abroad. The main benefit for Latvian academic organisations (e.g. RTU) joining X-Road are cross-border collaboration opportunities. RTU is a state-funded university in Latvia which is also active in providing e-infrastructure services at a national level, like HPC and data storage. RTU HPC infrastructure currently is the main place for processing and storing biomedical scientific data in Latvia (e.g. genome data), therefore data security and exchange of sensitive information is of a particular interest. There have also been efforts in Latvia under the Ministry of Environmental Protection and Regional Development regarding exchange of state information but the current solutions are not as widely adapted as X-Road and don't have focus on secure information exchange. Recently the DAGR project [https://www.varam.gov.lv/lv/projekts/projekts-datu-izplatisanas-un-parvaldibas-platforma-dagr] has been launched in Latvia which promises to improve information exchange and interoperability of services in the governmental sector.

The organisations from Latvia or other countries that are willing to subscribe for X-Road service and maintain their own Security Server (gateway) can join X-Road under the Estonian environment. For that the organisation should appoint the representative who will be authorized to sign a service contract as well as perform other administrative tasks on behalf of the organisation. The current limitation is that only a person with an Estonian ID can access the X-Road self-service environment because foreign electronic identity verification is not fully

operational. So there are two choices: the organisation can authorise it's employee who is an Estonian resident or somebody from the organisation applies for Estonian e-residency[26].

For RTU to join the X-Road, the second option was preferred, and an employee of the university applied for e-residency to obtain an Estonian ID card, hence also an ID code and e-signature. The whole formal process for RTU registration in X-Road can be divided into three steps:

- application for Estonian e-residency;
- preparation of an authorization letter;
- signing X-Road service subscription contract.

The application for e-residency is well organised and most of it can be performed remotely through https://eresident.politsei.ee/, although some effort is needed to fill out the application form and justify your intention to become e-resident. The whole process from filling the application until its approval and issuance of ID card in person in the Estonian Embassy took around 1 month.

Secondly, it was necessary to obtain the authorization letter which authorised the employee to represent RTU in X-Road. In addition RIA must make sure that the letter is signed by someone with the legal right to represent the organization (director general or member of the board). Usually it is verified by looking at the online business registry as it lists the board members who have this right. In the case of RTU, the only person who fulfils these requirements is the rector of the university. For larger organisations as in the case of RTU the process takes a few days because the letter must be verified by the legal department and then might wait in queue to be electronically signed by the rector.

In the last step, a service subscription contract must be signed. Since this is done by the person who is already authorized by the organisation, it takes the least effort. After signing the contract, the organisation is added to the X-Road registry and the authorised person's account is linked to the organisation. The account is accessible through X-Road self-service portal (dashboard) https://x-tee.ee/ by using an ID-card for authentication.

### 5.6.1 Deploying X-Road software

X-Road software deployment at RTU consisted of two components:

- X-Road Security Server - the main X-Road gateway for RTU
- Client service (GenData) which provides access to data over X-Road

The Security Server installation and configuration was done according to the online guide https://abi.ria.ee/xtee/en/turvaserveri-haldus/turvaserveri-paigaldamine hosted by Estonian RIA. The configuration assumes that the Security Server owner is already a member of the X-Road which means that the process described in the section 3.3.1 (Joining X-Road) was fulfilled . The main steps involved are:

[26] https://learn.e-resident.gov.ee/hc/en-us/articles/360000625098-Why-become-an-e-resident

- Preparation of a virtual machine: 2 virtual CPU cores, 4G RAM and 30 GB disk space, Ubuntu 20.04.2 LTS which is officially supported operating system by RIA, public network IP which is registered domain x-road.hpc.rtu.lv.
- Installation of X-Road packages (ver.6);
- Configuration of the Security Server through graphical admin interface https://x-road.hpc.rtu.lv:4000;
- Obtaining certificates - authentication and signing  keys for the Security Server.
- Adding subsystem (client). Subsystem “vooWeep6” was added (figure).
- Registering a subsystem in the central x-road dashboard.

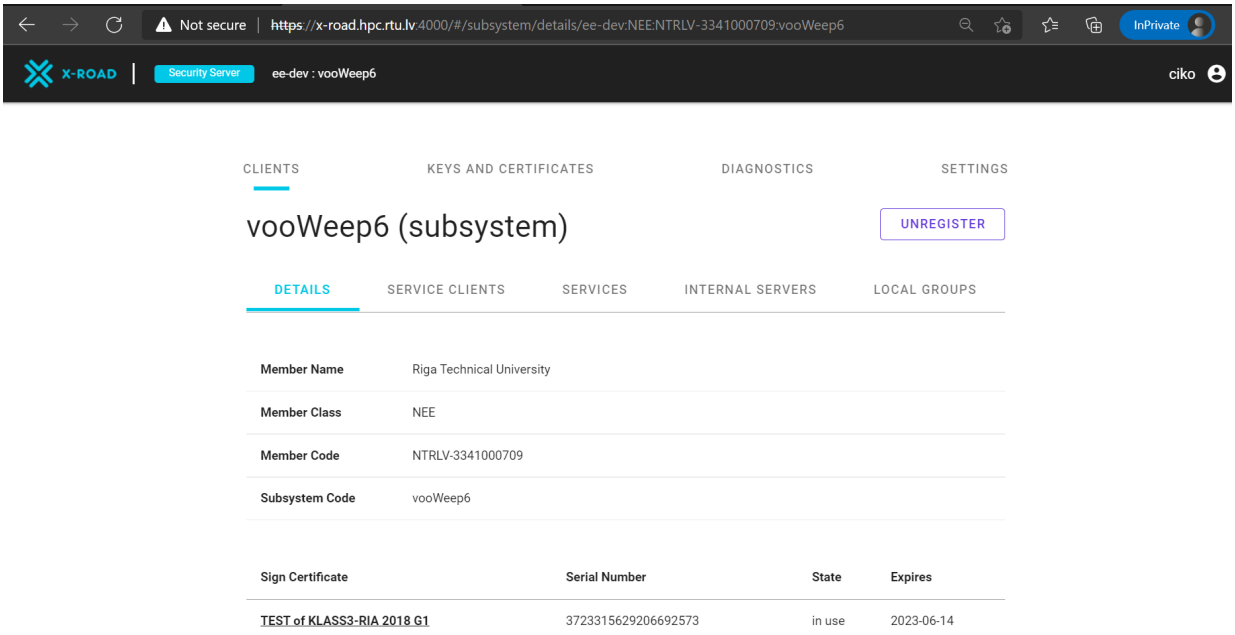



*Figure 13 X-Road subsystem exposing GenMed Genetic Data Repository in RTU.*

The subsystems added to the Security Server must be registered in the central X-Road dashboard https://x-tee.ee/dashboard. The dashboard is also used to sign certificate requests (keys) for the Security Server (only for test and development environments). Central dashboard can be accessed by authenticating with an ID-card which was received by the RTU representative. Example of the interface and subsystem “vooWeep6” registered for RTU:

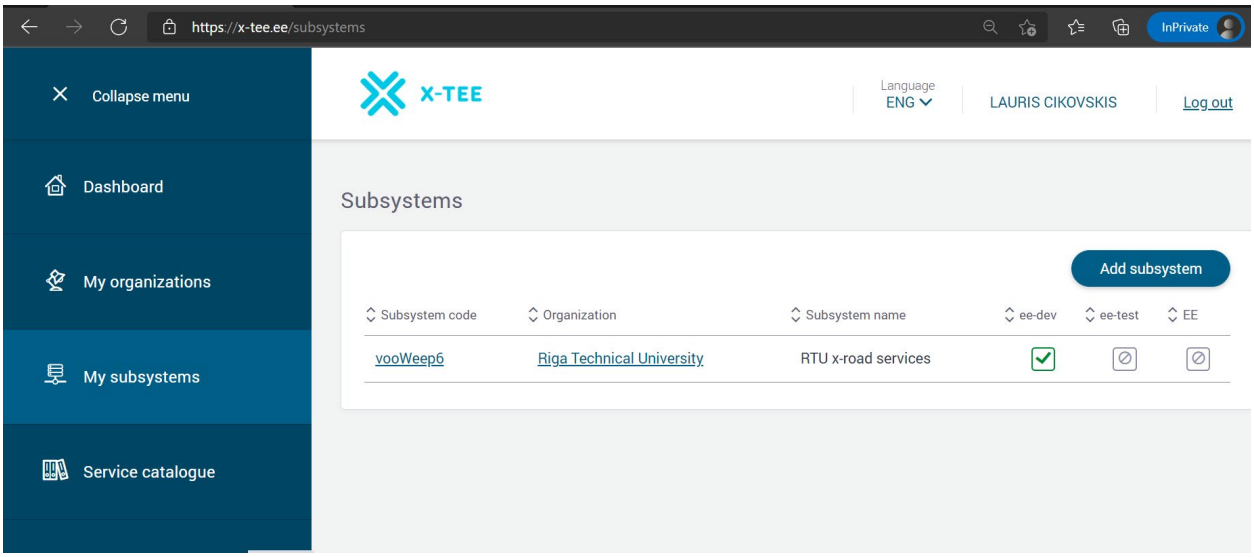



*Figure 14 Self-service of X-Road in Estonian deployment (X-Tee). The self-service is integrated with Estonina national catalogue of services (RIHA).*

The client service GenData is deployed in the same cloud infrastructure and the same subnetwork as the Security Server. A separate virtual server is used with the following parameters:

- 2 virtual CPU cores, 4G RAM and 20 GB disk space;
- Linux Centos 7.9 operating system.

In the current setup which is proof-of-the concept, there is no need to provide direct public access to the GenData service. All data input/output operations are performed through X-Road Security Server. The network topology of service deployment at RTU is shown in the next figure.

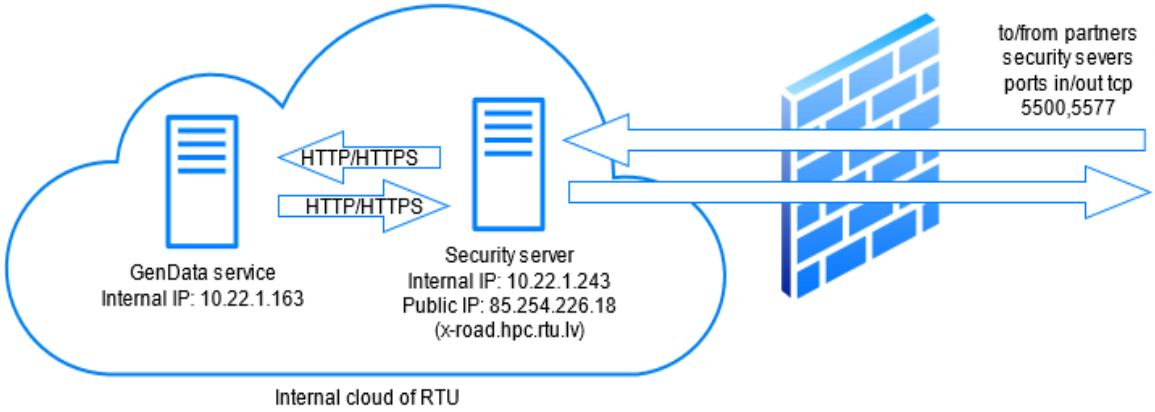



*Figure 15 Overview of deployment of GenData with X-Road Security Server in RTU.*

# 6 Next steps

During the first phase of the evaluation of X-Road, a lot of effort went into understanding better the governance structure, implications as well as setting up a basic prototype.

For our second phase, we are considering evaluating three additional aspects:

- Introduction and connection of another service from the same data domain as GenMed, but not aware of X-Road. The goal is to get practical experience about the amount of effort required for integration with X-Road of an existing application.
- Understanding better implications of reusing existing service – e.g. GenData – for other service clients. In particular, what legal and organizational steps would need to be taken. The goal is to understand if X-Road increases or decreases the effort for establishing collaborations with new clients.
- Finally, we plan to compare the service delivery model in X-Road with that of EOSC.

# 7 Appendix A

## 7.1 Example of X-Road Security Server configuration

To provide a better overview about the steps required for setting up federation of a service across the border, we provide screenshots of the web interface of the Estonian X-Road Security Server in the Development environment with the main sections.

### 7.1.1 List of X-Road clients and their subsystems

The X-Road Security Server can serve potential multiple organizations, however in our setup we have 1 server per organization.

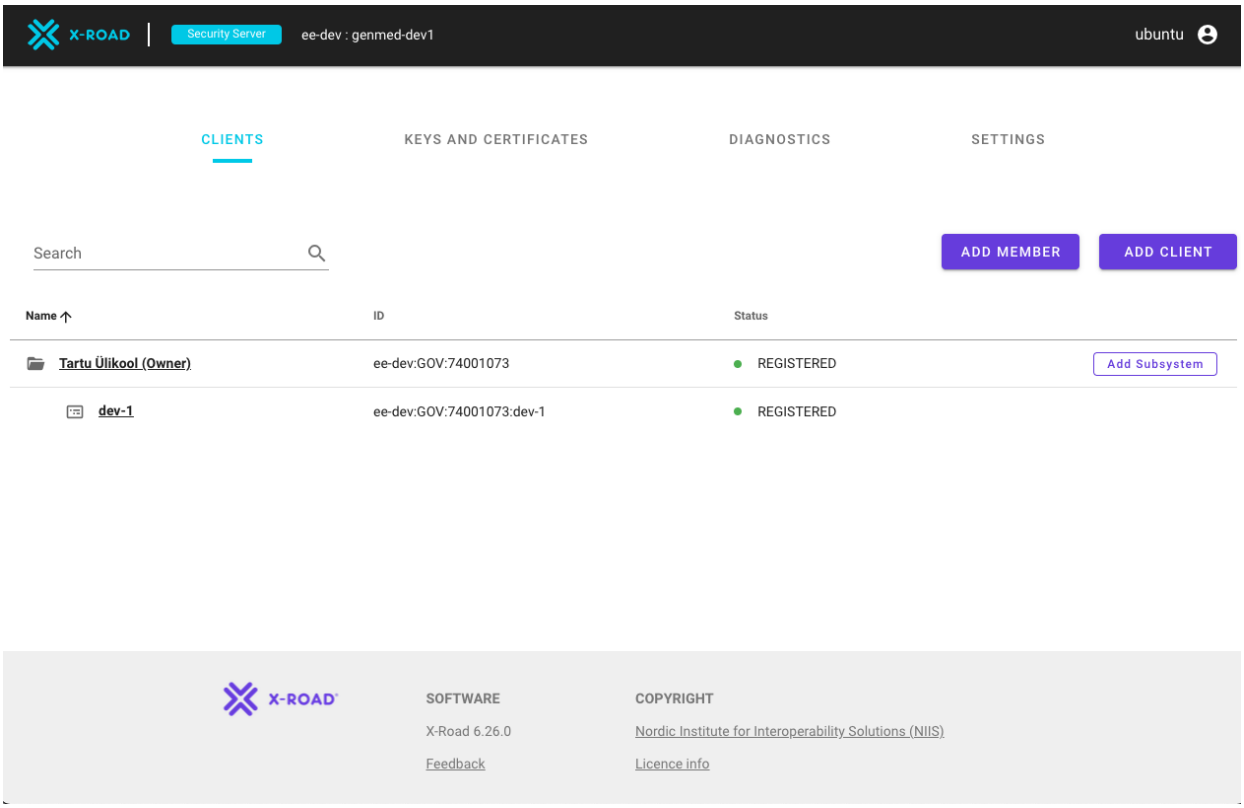



*Figure 16 List of X-Road clients in UT X-Road server for EOSC-Nordic*

### 7.1.2 Details of the subsystem

The subsystem corresponds to the informational system used for providing / accessing services via X-Road.

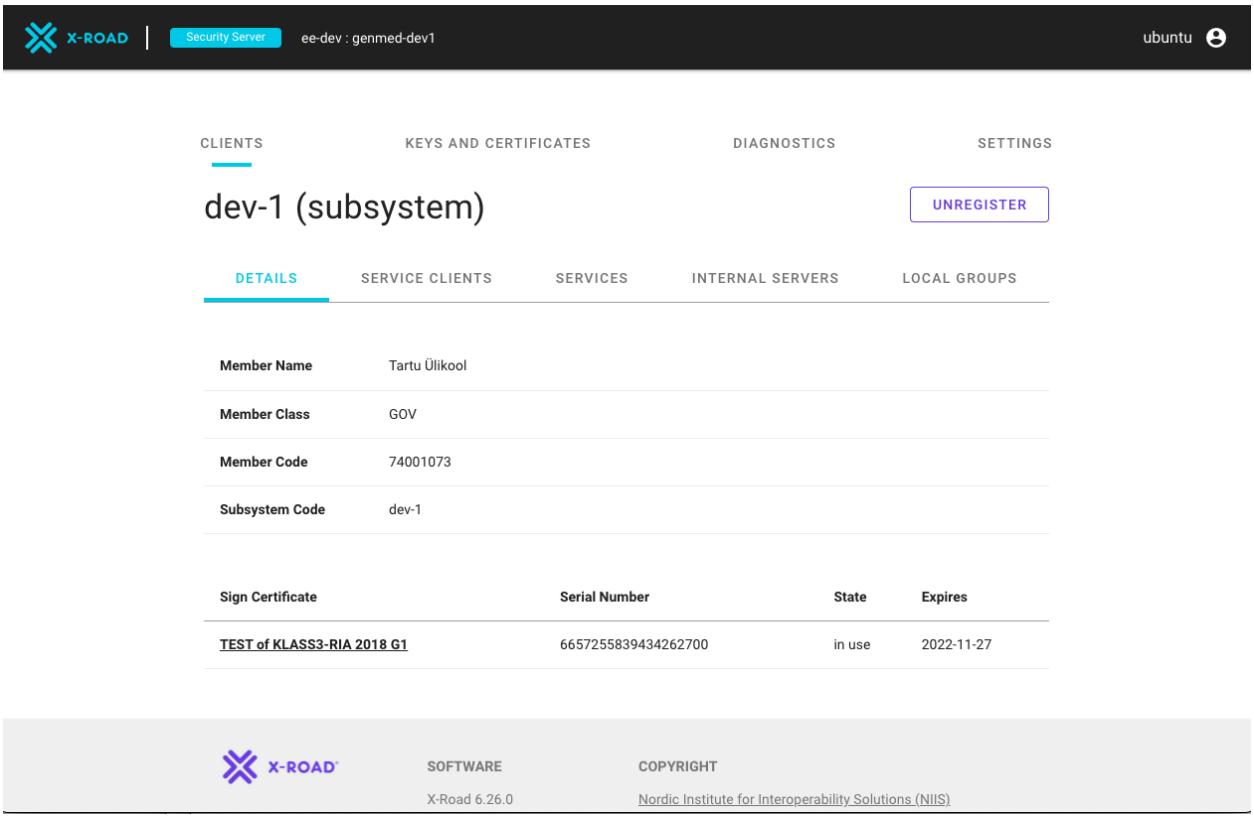



*Figure 17 Details of X-Road subsystem for GenData in UT.*

The subsystem can be authorized for access by other subsystems - service clients, including itself (e.g. if you have both service provider and consumer in the same organization). Service client list comes from the central registry.

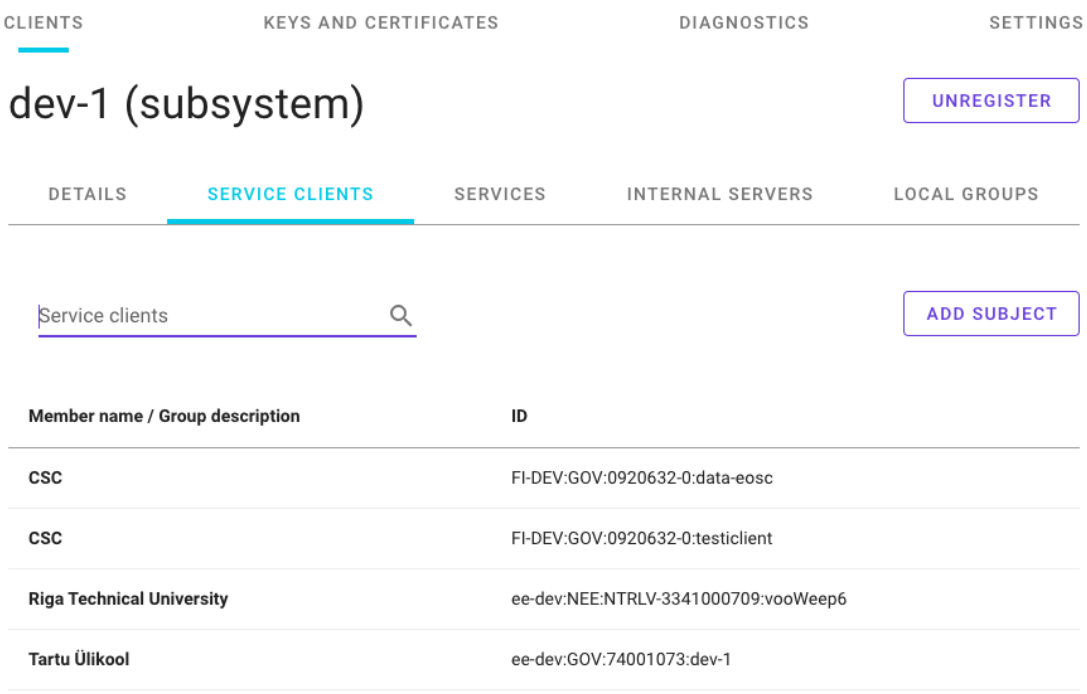



*Figure 18 List of clients for a subsystem, which exposes GenMed services in UT.*

### 7.1.3 Services of the subsystem

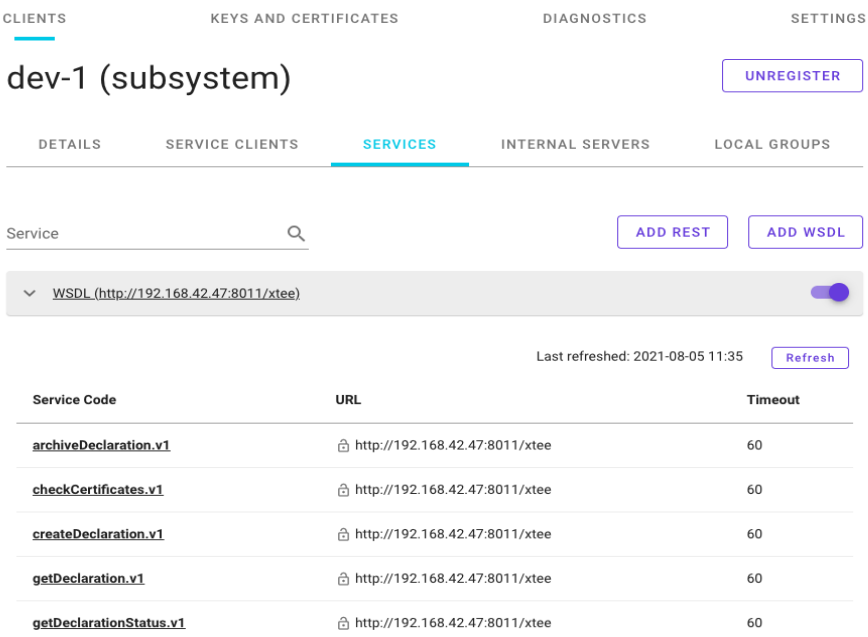



*Figure 19 List of specific services exposed by an information system in UT through X-Road*

Each specific service can be further configured with respect to how it is accessed (e.g. who and what is expected in the duration of the query processing).

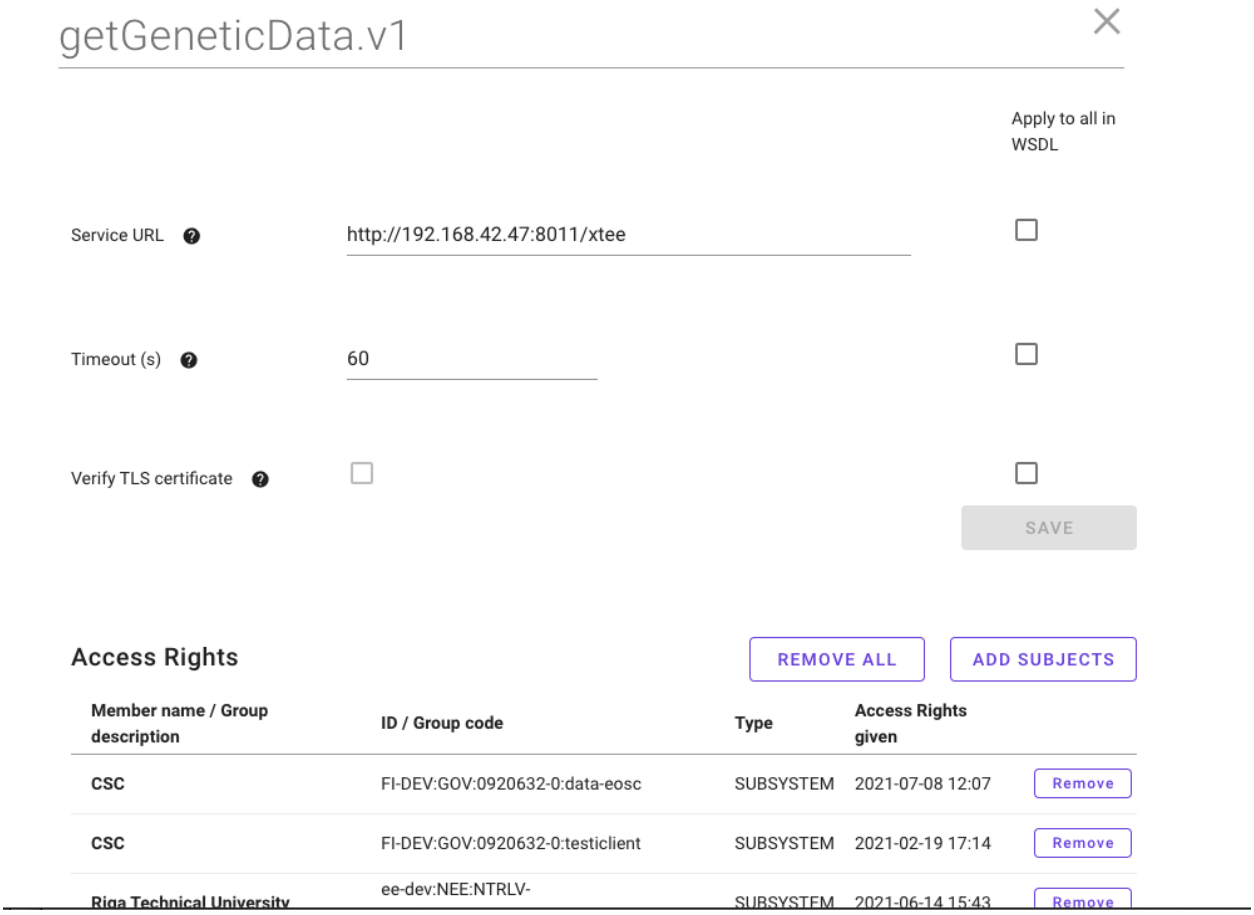



*Figure 20 Detail view of a specific service exposed via X-Road. Access rights as well as timeouts can be managed from this view.*

To authorize a new client to use the infosystem or a specific service, one can search for the client in the catalogue, optionally defining additional filters like type of the organization, represented by Member class field (e.g. GOV for state agency or COM commercial company), or accessible X-Road environment instance - either the one where the client has joined or one of the federated ones. In the screenshot below, FI-DEV corresponds to a Finnish development environment of X-Road, which is being trusted by the Security Server.

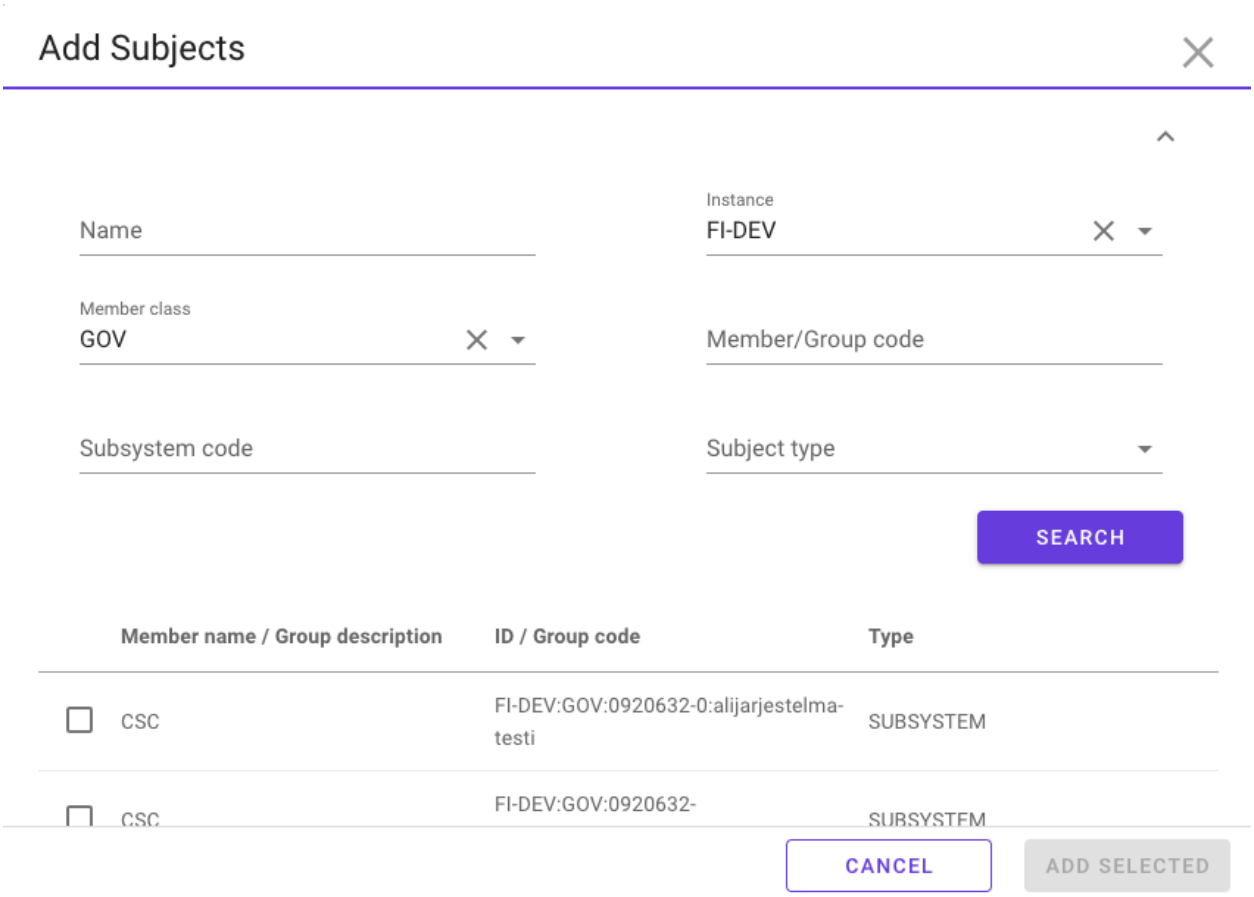



*Figure 21 Lookup of potential new clients of a service for authorization. Search is done across different environments trusted by the X-Road Security Server.*