

X-ROAD 6

SECURITY SERVER USER GUIDE

2.9

VERSION HISTORY

Date	Version	Description
05.09.2014	0.1	Initial draft
24.09.2014	0.2	Translation to English
10.10.2014	0.3	Update
14.10.2014	0.4	Title page, header, footer added
16.10.2014	0.5	Minor corrections done
12.11.2014	0.6	Asynchronous messages section removed. Global Configuration distributors section replaced with Configuration Anchor section (10.1). Added Logback information (Chapter 15). A note added about the order of timestamping services (Section 10.2).
1.12.2014	1.0	Minor corrections done
19.01.2015	1.1	License information added
27.01.2015	1.2	Minor corrections done
30.04.2015	1.3	“sdsb” changed to “xroad”
29.05.2015	1.4	Message Log chapter added (Chapter)
30.06.2015	1.5	Minor corrections done
3.07.2015	1.6	Audit Log chapter added (Chapter 12)
7.09.2015	1.7	Message Log – how to use remote database (Section 11.3)
14.09.2015	1.8	Reference to the audit log events added
18.09.2015	1.9	Minor corrections done
21.09.2015	2.0	References fixed
07.10.2015	2.1	Default value of the parameter <i>acceptable-timestamp-failure-period</i> set to 14400
14.10.2015	2.2	Instructions for using an external database for the message log corrected
05.11.2015	2.3	Updates related to backup and restore (Chapter 13)
30.11.2015	2.4	X-Road concepts updated (Section 1.2). Security server registration updated (Chapter 3). Security server clients updated (Chapter 4); only subsystems (and not members) can be registered as security server clients and have services or access rights configured. Cross-references fixed. Editorial changes made.

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

09.12.2015	2.5	Security server client deletion updated (Section 4.5.2). Editorial changes made.
14.12.2015	2.6	Message log updated (Chapter)
14.01.2016	2.7	Logs updated (Chapter 15)
08.02.2016	2.8	Corrections in chapter 15
20.05.2016	2.9	Merged changes from xtee6-doc repo. Added Chapter 14 Diagnostics and updated content of 10.3 Changing the Internal TLS Key and Certificate.

TABLE OF CONTENTS

1. Introduction.....	6
1.1. The X-Road Security Server.....	6
1.2. X-Road Concepts.....	6
1.3. References.....	8
2. User Management.....	9
2.1. User Roles.....	9
2.2. Managing the Users.....	9
3. Security Server Registration.....	10
3.1. <u>Configuring the Signing Key and Certificate for the Security Server Owner</u> 10	
3.1.1. <u>Generating a Signing Key</u>	10
3.1.2. <u>Generating a Certificate Signing Request for a Signing Key</u>	10
3.1.3. <u>Importing a Certificate from the Local File System</u>	11
3.1.4. <u>Importing a Certificate from a Security Token</u>	11
3.2. <u>Configuring the Authentication Key and Certificate for the Security Server</u> 12	
3.2.1. <u>Generating an Authentication Key</u>	12
3.2.2. <u>Generating a Certificate Signing Request for an Authentication Key</u> ..	12
3.2.3. <u>Importing an Authentication Certificate from the Local File System</u> ...	13
3.3. <u>Registering the Security Server in the X-Road Governing Authority</u>	13
3.3.1. <u>Registering an Authentication Certificate</u>	13
4. Security Server Clients.....	14
4.1. <u>Security Server Client States</u>	14
4.2. <u>Adding a Security Server Client</u>	15
4.3. <u>Configuring a Signing Key and Certificate for a Security Server Client</u>	15
4.4. <u>Registering a Security Server Client in the X-Road Governing Authority</u> ...	16
4.4.1. <u>Registering a Security Server Client</u>	16
4.5. <u>Deleting a Client from the Security Server</u>	16
4.5.1. <u>Unregistering a Client</u>	17
4.5.2. <u>Deleting a Client</u>	17
5. Security Tokens, Keys, and Certificates.....	18
5.1. <u>Availability States of Security Tokens, Keys, and Certificates</u>	18
5.2. <u>Registration States of Certificates</u>	18

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

5.2.1.	Registration States of the Signing Certificate	18
5.2.2.	Registration States of the Authentication Certificate	18
5.3.	Validity States of Certificates	20
5.4.	Activating and Disabling the Certificates	20
5.5.	Configuring and Registering an Authentication key and Certificate	20
5.6.	Deleting a Certificate	21
5.6.1.	Unregistering an Authentication Certificate	21
5.6.2.	Deleting a Certificate or a certificate Signing Request notice	21
5.7.	Deleting a Key	22
6.	X-Road Services	23
6.1.	Adding a WSDL	23
6.2.	Refreshing a WSDL	23
6.3.	Enabling and Disabling a WSDL	24
6.4.	Changing the Address of a WSDL	24
6.5.	Deleting a WSDL	24
6.6.	Changing the Parameters of a Service	25
7.	Access Rights	26
7.1.	Changing the Access Rights of a Service	26
7.2.	Adding a Service Client	26
7.3.	Changing the Access Rights of a Service Client	27
8.	Local Access Right Groups	28
8.1.	Adding a Local Group	28
8.2.	Displaying and Changing the Members of a Local Group	28
8.3.	Changing the description of a Local Group	28
8.4.	Deleting a Local Group	29
9.	Communication with the Client Information Systems	30
10.	System Parameters	32
10.1.	Managing the Configuration Anchor	32
10.2.	Managing the Timestamping Services	32
10.3.	Changing the Internal TLS Key and Certificate	33
11.	Message Log	35
11.1.	Changing the Configuration of the Message Log	35
11.1.1.	Common parameters	36
11.1.2.	Timestamping parameters	36

11.1.3. Archiving parameters	36
11.2. Transferring the Archive Files from the Security Server	36
11.3. Using a Remote Database	38
12. Audit Log	40
12.1. Changing the Configuration of the Audit Log	40
12.2. Archiving the Audit Log	41
13. Back up and Restore	42
13.1. Back up and Restore in the User Interface	42
13.2. Restore from the Command Line	42
14. Diagnostics	44
14.1. Examine security server services status information	44
15. Logs and System Services	45
15.1. System Services	45
15.2. Logging configuration	45
15.3. Fault Detail UUID	46

1. INTRODUCTION

This document describes the management and maintenance of an X-Road version 6 security server.

1.1. THE X-ROAD 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. In a sense, the security server can be seen as a specialized application-level firewall that supports the SOAP protocol; hence, it should be set up in parallel with the organization's firewall, which mediates other protocols.

The security server is equipped with the functionality needed to secure the message exchange between a client and a service provider.

- Messages transmitted over the public Internet are secured using digital signatures and encryption.
- The service provider's security server applies access control to incoming messages, thus ensuring that only those users that have signed an appropriate agreement with the service provider can access the data.

To increase the availability of the entire system, the service user's and service provider's security servers can 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 between the security servers.
- If one of the service provider's security servers goes offline, the requests are automatically redirected to other available security servers.

The security server also depends on a central server, which provides the global configuration.

1.2. X-ROAD CONCEPTS

- **Global configuration** consists of XML files, which are regularly downloaded by security servers from the X-Road central server. The global configuration includes, among other data, the following:
 - o the addresses and public keys of trust anchors (certification service CAs and timestamping services);
 - o the public keys of intermediate CAs;

- o the addresses and public keys of OCSP services (if not already available through the certificates' *Authority Information Access* extension);
 - o information about X-Road members and their subsystems;
 - o the addresses of the members' security servers registered in X-Road;
 - o information about the security servers' authentication certificates registered in X-Road;
 - o information about the security servers' clients registered in X-Road;
 - o information about global access rights groups;
 - o X-Road system parameters.
- **Member class** groups X-Road members with similar properties under a common unit. E.g., state agencies are grouped under the member class "GOV", private organizations are grouped under the member class "COM", etc.
 - **Member code**, associated uniquely with a certain X-Road member, is a unique character combination within its particular member class. The member code remains unchanged during the entire lifetime of the member. For example, the member code for organizations and state agencies in Estonia is the Business Registry code.
 - **Security server client** is a subsystem of an X-Road member, whose association with a security server is registered in the X-Road governing authority and that uses the security server for using and/or providing X-Road services.
 - **Security server owner** is an X-Road member legally responsible for a particular security server. The security server owner is displayed in the list of security server clients ("Configuration" -> "Security Server Clients") in bold font style.
 - **Subsystem** represents a part of an X-Road member's information system. X-Road members must declare parts of its information system as subsystems to use or provide X-Road services.

Subsystems are autonomous in terms of providing and using X-Road services.

- o The access rights of an X-Road members' subsystems are independent – access rights given to one subsystem do not affect the access rights of the members' other subsystems.
- o Services provided by a subsystem are independent of the services provided by the members' other subsystems.

To sign the messages sent by a subsystem when using or providing X-Road services, the signing certificate of the member that manages the subsystem is used. An X-Road member can associate several different subsystems with

one security server, and one subsystem can be associated with several security servers.

- **X-Road certificate** is issued by a certification service provider that has been approved in the X-Road governing authority. An X-Road certificate is either:
 - a **signing certificate**, which is issued to X-Road members and which the security servers use to digitally sign the mediated data or
 - an **authentication certificate**, which is issued to security servers and which is used to establish the secure communications channel between security servers.
- **X-Road instance** identifier helps to distinguish between different X-Road instances. Each instance is assigned an identifying code. E.g. the code for the Estonian development instance is “ee-dev” and the code for production instance is “EE”.
- **X-Road member** is a legal (or physical) person who has joined the X-Road and uses the functionality provided by the X-Road in the capability of service provider and/or user.
- **X-Road messages** are service requests and responses described according to the X-Road Message Protocol (see [PR-MESS]), that are exchanged between the information systems using or providing services and the security servers.

1.3. REFERENCES

1. [ASiC] ETSI TS 102 918, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
2. [CRON] Quartz Scheduler CRON expression, http://www.quartz-scheduler.org/generated/2.2.1/html/qs-all/#page/Quartz_Scheduler_Documentation_Set%2Fcotrg_crontriggers.html
3. [INI] INI file, http://en.wikipedia.org/wiki/INI_file
4. [JDBC] Connecting to the Database, <https://jdbc.postgresql.org/documentation/93/connect.html>
5. [JSON] Introducing JSON, <http://json.org/>
6. [PR-MESS] Cybernetica AS. X-Road: Message Protocol v4.0. Document ID: PR-MESS
7. [SPEC-AL] Cybernetica AS. X-Road: Audit log events. Document ID: SPEC-AL

2. USER MANAGEMENT

2.1. USER ROLES

Security servers support the following user roles:

- **Security Officer** (xroad-security-officer) is responsible for the application of the security policy and security requirements, including the management of key settings, keys, and certificates.
- **Registration Officer** (xroad-registration-officer) is responsible for the registration and removal of security server clients.
- **Service Administrator** (xroad-service-administrator) manages the data of and access rights to services
- **System Administrator** (xroad-system-administrator) is responsible for the installation, configuration, and maintenance of the security server.

One user can have multiple roles and multiple users can be in the same role. Each role has a corresponding system group, created upon the installation of the system.

Henceforth each applicable section of the guide indicates, which user role is required to perform a particular action. For example:

Access rights: Security Officer

If the logged-in user does not have a permission to carry out a particular task, the button that would initiate the action is hidden (and neither is it possible to run the task using its corresponding keyboard combinations or mouse actions). Only the permitted data and actions are visible and available to the user.

2.2. MANAGING THE USERS

User management is carried out on command line in root user permissions.

To add a new user, enter the command:

```
adduser username
```

To grant permissions to the user you created, add it to the corresponding system groups, for example:

```
adduser username xroad-security-officer
adduser username xroad-registration-officer
adduser username xroad-service-administrator
adduser username xroad-system-administrator
```

To remove a user permission, remove the user from the corresponding system group, for example:

```
deluser username xroad-security-officer
```

To remove a user, enter:

*This work is licensed under the Creative Commons Attribution-ShareAlike 3.0
Unported License. To view a copy of this license, visit
<http://creativecommons.org/licenses/by-sa/3.0/>*

deluser username

3. SECURITY SERVER REGISTRATION

To use a security server for mediating (exchanging) messages, the security server and its owner must be certified by a certification service provider approved by the X-Road governing authority, and the security server has to be registered in the X-Road governing authority.

3.1. CONFIGURING THE SIGNING KEY AND CERTIFICATE FOR THE SECURITY SERVER OWNER

The signing keys used by the security servers for signing X-Road messages can be stored on software or hardware based (a Hardware Security Module or a smartcard) security tokens, according to the security policy of the X-Road instance.

Depending on the certification policy, the signing keys are generated either in the security server or by the certification service provider. Sections 3.1.1 to 3.1.3 describe the actions necessary to configure the signing key and certificate in case the key is generated in the security server. Section 3.1.4 describes the importing of the signing key and certificate in case the key is generated by the certification service provider.

The **background colors** of the devices, keys and certificate are explained in Section 5.1.

3.1.1. GENERATING A SIGNING KEY

Access rights:

- All activities: Security Officer
- All activities except logging into the key device: Registration Officer
- Logging in to the key device: System Administrator

To generate a signing key, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. If you are using a hardware security token, ensure that the device is connected to the security server. The device information must be displayed in the **Keys and Certificates** table.
3. To log in to the token, click **Enter PIN** on the token's row in the table and enter the PIN code. Once the correct PIN is entered, the **Enter PIN** button changes to **Logout**.
4. To generate a signing key, select the token from the table by clicking the respective row, and click **Generate key**. Enter the label value for the key and click **OK**. The generated key appears under the token's row in the table. The label value is displayed as the name of the key.

3.1.2. GENERATING A CERTIFICATE SIGNING REQUEST FOR A SIGNING KEY

Access rights: Security Officer, Registration Officer

To generate a certificate signing request (CSR) for the signing key, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. Select a key from the table and click **Generate CSR**. In the dialog that opens
 - 2.1. Select the certificate usage policy from the **Usage** drop down list (SIGN for signing certificates);
 - 2.2. select the X-Road member the certificate will be issued for from the **Client** drop-down list;
 - 2.3. select the issuer of the certificate from the **Certification Service** drop-down list;
 - 2.4. select the format of the certificate signing request (PEM or DER), according to the certification service provider's requirements
 - 2.5. click **OK**;
3. In the form that opens, review the certificate owner's information that will be included in the CSR and fill in the empty fields, if needed.
4. Click **OK** to complete the generation of the CSR and save the prompted file to the local file system.

After the generation of the CSR, a "Request" record is added under the key's row in the table, indicating that a certificate signing request has been created for this key. The record is added even if the request file was not saved to the local file system.

To certify the signing key, transmit the certificate signing request to the approved certification service provider and accept the signing certificate created from the certificate signing request.

3.1.3. IMPORTING A CERTIFICATE FROM THE LOCAL FILE SYSTEM

Access rights: Security Officer, Registration Officer

To import the signing certificate to the security server, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. Click **Import certificate**.
3. Locate the certificate file from the local file system and click **OK**. After importing the certificate, the "Request" record under the signing key's row is replaced with the information from the imported certificate. By default, the signing certificate is imported in the "Registered" state.

3.1.4. IMPORTING A CERTIFICATE FROM A SECURITY TOKEN

Access rights: Security Officer, Registration Officer

To import a certificate from a security token, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. Make sure that a key device containing the signing key and the signing certificate is connected to the security server. The device and the keys and certificates stored on the device must be displayed in the **Keys and Certificates** view.
3. To log in to the security token, click **Enter PIN** on the token's row in the table and enter the PIN. Once the correct PIN is entered, the **Enter PIN** button changes to **Logout**.
4. Click the **Import** button on the row of the certificate. By default, the certificate is imported in the "Registered" state.

3.2. CONFIGURING THE AUTHENTICATION KEY AND CERTIFICATE FOR THE SECURITY SERVER

The **background colors** of the devices, keys and certificate are explained in Section 5.1.

3.2.1. GENERATING AN AUTHENTICATION KEY

Access rights

- All activities: Security Officer
- Logging in to the key device: System Administrator

The security server's authentication keys can only be generated on software security tokens.

1. On the **Management** menu, select **Keys and Certificates**.
2. To log in to the software token, click **Enter PIN** on the token's row in the table and enter the token's PIN code. Once the correct PIN is entered, the **Enter PIN** button changes to **Logout**.
3. To generate an authentication key, select the software token from the table by clicking the respective row, and click **Generate key**. Enter the label value for the key and click **OK**. The generated key appears under the token's row in the table. The label value is displayed as the name of the key.

3.2.2. GENERATING A CERTIFICATE SIGNING REQUEST FOR AN AUTHENTICATION KEY

Access rights: Security Officer

To generate a certificate signing request (CSR) for the authentication key, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

2. Select the authentication key from the table and click **Generate CSR**. In the dialog that opens
 - 2.1. Select the certificate usage policy from the **Usage** drop down list (AUTH for authentication certificates);
 - 2.2. select the issuer of the certificate from the **Certification Service** drop-down list;
 - 2.3. select the format of the certificate signing request (PEM or DER), according to the certification service provider's requirements
 - 2.4. click **OK**;
3. In the form that opens, review the information that will be included in the CSR and fill in the empty fields, if needed.
4. Click **OK** to complete the generation of the CSR and save the prompted file to the local file system.

After the generation of the CSR, a "Request" record is added under the key's row in the table, indicating that a certificate signing request has been created for this key. The record is added even if the request file was not saved to the local file system.

To certify the authentication key, transmit the certificate signing request to the approved certification service provider and accept the authentication certificate created from the certificate signing request.

3.2.3. IMPORTING AN AUTHENTICATION CERTIFICATE FROM THE LOCAL FILE SYSTEM

Access rights: Security Officer

To import the authentication certificate to the security server, follow these steps.

1. On the Management menu, select Keys and Certificates.
8. Click Import certificate.
9. Locate the certificate file from the local file system and click OK. After importing the certificate, the "Request" record under the authentication key's row is replaced with the information from the imported certificate. By default, the certificate is imported in the "Saved" (see Section 5.2.2) and "Disabled" states (see Section 5.3).

3.3. REGISTERING THE SECURITY SERVER IN THE X-ROAD GOVERNING AUTHORITY

To register the security server in the X-Road governing authority, the following actions must be completed.

- The authentication certificate registration request must be submitted from the security server (see 3.3.1).

- A request for registering the security server must be submitted to the X-Road governing authority according to the organizational procedures of the X-Road instance.
- The registration request must be approved by the X-Road governing authority.

3.3.1. REGISTERING AN AUTHENTICATION CERTIFICATE

Access rights: Security Officer

The security server's registration request is signed in the security server with the server owner's signing key and the server's authentication key. Therefore, ensure that the corresponding certificates are imported to the security server and are in a usable state (the tokens holding the keys are in logged in state and the OCSP status of the certificates is "good").

To submit an authentication certificate registration request, follow these steps.

1. On the Management menu, select Keys and Certificates.
10. Select an authentication certificate to be registered (it must be in the "saved" state) and click **Register**.
11. In the dialog that opens, enter the security server's public DNS name or its external IP address and click **OK**.

On submitting the request, the message "Request sent" is displayed, and the authentication certificate's state is set to "Registration in process".

After the X-Road governing authority has accepted the registration, the registration state of the authentication certificate is set to "Registered" and the registration process is completed.

4. SECURITY SERVER CLIENTS


Important: to use or provide X-Road services, a security server client needs to be certified by a certification service provider approved by the X-Road governing authority, and the association between the client and the security server used by the client must be registered at the X-Road governing authority.

This section does not address managing the owner to a security server. The owner's information has been already added to the security server upon the installation, and registered upon the security server's registration. The owner's registration status can be looked up by selecting **Security Server Clients** on the **Configuration** menu. The security server's owner is displayed in bold. Before the registration of the security server, the owner is in the "Saved" state and after the completion of the registration process, in the "Registered" state.


The registration of the security server's owner does not extend to the owner's subsystems. The subsystems must be registered as individual clients.

4.1. SECURITY SERVER CLIENT STATES


The security server distinguishes between the following client states.

 **Saved** – the client's information has been entered and saved into the security server's configuration (see 4.2), but the association between the client and the security server is not registered in the X-Road governing authority. (If the association is registered in the central server prior to the entry of data, the client will move to the "Registered" state upon data entry.) From this state, the client can move to the following states:

- "Registration in progress", if a registration request for the client is submitted from the security server (see 4.4.1);
- "Deleted", if the client's information is deleted from the security server configuration (see 4.5.2).


 **Registration in progress** – a registration request for the client is submitted from the security server to the central server, but the association between the client and the security server is not yet approved by the X-Road governing authority. From this state, the client can move to the following states:

- "Registered", if the association between the client and the security server is approved by the X-Road governing authority (see 4.4.1);
- "Deletion in progress", if a client deletion request is submitted from the security server (see 4.5.1).


 **Registered** – the association between the client and the security server has been approved in the X-Road governing authority. In this state, the client can

provide and use X-Road services (assuming all other prerequisites are fulfilled). From this state, the client can move to the following states:

- "Global error", if the association between the client and the security server has been revoked by the X-Road governing authority;
- "Deletion in progress", if a client deletion request is submitted from the security server (see 4.5.1).

 **Global error** – the association between the client and the security server has been revoked in the central server. From this state, the client can move to the following states:

- "Registered", if the association between the client and the security server has been restored in the central server (e.g., the association between the client and the security server was lost due to an error);
- "Deleted", if the client's information is deleted from the security server's configuration (see 4.5.2).

 **Deletion in progress** – a client deletion request has been submitted from the security server. From this state, the client can move to the following state:

- "Deleted", if the client's information is deleted from the security server's configuration (see 4.5.2).

Deleted – the client's information has been deleted from the security server's configuration.

4.2. ADDING A SECURITY SERVER CLIENT

Access rights: Registration Officer

Follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**.
2. Click **Add Client**. In the window that opens, either enter the client's information manually or click **Select Client from Global List** and locate the client's information from within all X-Road members and their subsystems.
3. Click **OK** once the client's information has been entered.

The new client is added to the list of security server clients in the "Saved" state.

4.3. CONFIGURING A SIGNING KEY AND CERTIFICATE FOR A SECURITY SERVER CLIENT

A signing key and certificate must be configured for the security server client to sign messages exchanged over the X-Road.

Certificates are not issued to subsystems; therefore, the certificate of the subsystem's owner (that is, an X-Road member) is used for the subsystem.

All particular X-Road member's subsystems that are registered in the same security server use the same signing certificate for signing messages. Hence, if the security server already contains the member's signing certificate, it is not necessary to configure a new signing key and/or certificate when adding a subsystem of that member.

The process of configuring the signing key and certificate for a security server client is the same as for the security server owner. The process is described in Section 3.1.

4.4. REGISTERING A SECURITY SERVER CLIENT IN THE X-ROAD GOVERNING AUTHORITY

To register a security server client in the X-Road governing authority, the following actions must be completed.

- The security server client registration request must be submitted from the security server (see 4.4.1).
- A request for registering the client must be submitted to the X-Road governing authority according to the organizational procedures of the X-Road instance.
- The registration request must be approved by the X-Road governing authority.

4.4.1. REGISTERING A SECURITY SERVER CLIENT

Access rights: Registration Officer

To submit a client registration request follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**.
2. Select the client in the "Saved" state from the list of security server clients.
3. Click the **Details** icon and in the window that opens, click **Register**.
4. Click **Confirm** to submit the request.

On submitting the request, the message "Request sent" is displayed, and the client's state is set to "Registration in process".

After the X-Road governing authority has accepted the registration, the state of the client is set to "Registered" and the registration process is completed.

4.5. DELETING A CLIENT FROM THE SECURITY SERVER

If a client is deleted from the security server, all the information related to the client is deleted from the server as well – that is, the WSDLs, services, access rights, and, if necessary, the certificates.

When one of the clients is deleted, it is not advisable to delete the signing certificate if the certificate is used by other clients registered to the security server, e.g., other subsystems belonging the same X-Road member as the deleted subsystem.

A client registered or submitted for registration in the X-Road governing authority (indicated by the "Registered" or "Registration in progress" state) must be unregistered before it can be deleted. The unregistering event sends a security server client deletion request from the security server to the central server.

4.5.1. UNREGISTERING A CLIENT

Access rights: Registration Officer

To unregister a client, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**.
2. Select the client that you wish to remove from the server and click the **Details** icon on the client's row.
3. In the window that opens, click **Unregister** and then click **Confirm**. The security server automatically sends a client deletion request to the X-Road central server, upon the receipt of which the association between the security server and the client is revoked.
4. Next, a notification is displayed about sending a deletion request to the central server, and a confirmation is presented about deleting the client's information (except its certificates).
 - If you wish to delete the client's information immediately, click **Confirm**. Next, an option is presented to delete the client's certificates. To delete the certificates, click **Confirm** again.
 - If you wish to retain the client's information, click **Cancel**. In that case, the client is moved to the "Deletion in progress" state, wherein the client cannot mediate messages and cannot be registered again in the X-Road governing authority.
5. To delete the information of a client in the "Deletion in progress" state, select the client by clicking the **Details** icon on its row, click **Delete** in the window that opens, and then click **Confirm**.

Note: It is possible to unregister a registered client from the central server without sending a deletion request through the security server. In this case, the security server's administrator responsible for the client must transmit a request containing information about the client to be unregistered to the central server's administrator. If the client has been deleted from the central server without a prior deletion request from the security server, the client is shown in the "Global error" state in the security server.

4.5.2. DELETING A CLIENT

Access rights: Registration Officer

A security server client can be deleted if its state is "Saved", "Global error" or "Deletion in progress". Clients that are in states "Registered" or "Registration in progress" need to be unregistered before they can be deleted (see Section 4.5.1).

To delete a client, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**.
2. Select from the table a client that you wish to remove from the security server and click the **Details** icon on that row.
3. In the window that opens, click **Delete**. Confirm the deletion by clicking **Confirm**.

5. SECURITY TOKENS, KEYS, AND CERTIFICATES

5.1. AVAILABILITY STATES OF SECURITY TOKENS, KEYS, AND CERTIFICATES

To display the availability of objects (that is, tokens, keys or certificates), the following background colors are used in the "Keys and Certificates" view.

- **Yellow** background – the object is available to the security server, but the object's information has not been saved to the security server configuration. For example, a smartcard could be connected to the server, but the certificates on the smartcard may not have been imported to the server. Certificates on the yellow background cannot be used for mediating messages.
- **White** background – the object is available to the security server and the object's information has been saved to the security server's configuration. **Certificates on the white background can be used for mediating messages.**
- **Gray** background – the object is not available for the security server. Certificates on the gray background cannot be used for mediating messages.

Caution: The key device's and key's information is automatically saved to the configuration when a certificate associated with either of them is imported to the security server, or when a certificate signing request is generated for the key. Similarly, the key device's and key's information is deleted from the security server configuration automatically upon the deletion of the last associated certificate and/or certificate signing request.

5.2. REGISTRATION STATES OF CERTIFICATES

Registration states indicate if and how a certificate can be used in the X-Road system. In the "Keys and Certificates" view, a certificate's registration states (except "Deleted") are displayed in the "Status" column.

5.2.1. REGISTRATION STATES OF THE SIGNING CERTIFICATE

A security server signing certificate can be in one of the following registration states.

- **Registered** – the certificate has been imported to the security server and saved to its configuration. A signing certificate in a "Registered" state can be used for signing X-Road messages.
- **Deleted** – the certificate has been deleted from the server configuration. If the certificate is in the "Deleted" state and stored on a hardware key device

connected to the security server, the certificate is displayed on a yellow background.

5.2.2. REGISTRATION STATES OF THE AUTHENTICATION CERTIFICATE

A security server authentication certificate can be in one of the following registration states.

Saved – the certificate has been imported to the security server and saved to its configuration, but the certificate has not been submitted for registration. From this state, the certificate can move to the following states:

- "Registration in progress", if the authentication certificate registration request is sent from the security server to the central server (see 3.3.1);
- "Deleted", if the authentication certificate's information is deleted from the security server configuration (see Section 5.6).

Registration in progress – an authentication certificate registration request has been created and sent to the central server, but the association between the certificate and the security server has not yet been approved. From this state, the certificate can move to the following states:

- "Registered", if the association between the authentication certificate and the security server is approved by the X-Road governing authority (see 3.3);
- "Deletion in progress", if the certificate deletion request has been submitted to the central server (see 5.6.1). The user can force this state transition even if the sending of the authentication certificate deletion request fails.

Registered – the association between the authentication certificate and the security server has been approved in the central server. An authentication certificate in this state can be used to establish a secure data exchange channel for exchanging X-Road messages. From this state, the certificate can move to the following states:

- "Global error", if the association between the authentication certificate and the security server has been revoked in the central server;
- "Deletion in progress", if the certificate deletion request has been transmitted to the central server (see 5.6.1). The user can force this state transition even if the sending of the authentication certificate deletion request fails.

Global error – the association between the authentication certificate and the security server has been revoked in the central server. From this state, the certificate can move to the following states:

- "Registered", if the association between the authentication certificate and the security server has been restored in the central server (e.g., the

association between the client and the security server was lost due to an error);

- "Deleted", if the authentication certificate's information is deleted from the security server configuration (see 5.6).

Deletion in progress – an authentication certificate registration request has been created for the certificate and sent to the central server. From this state, the certificate can move to the following state:

- "Deleted", if the authentication certificate's information is deleted from the security server configuration (see 5.6).

Deleted – the certificate has been deleted from the security server configuration.

5.3. VALIDITY STATES OF CERTIFICATES

Validity states indicate if and how a certificate can be used independent of the X-Road system. In the "Keys and Certificates" view, the certificate's validity states are displayed in the "OCSP response" column. Validity states (except "Disabled") are displayed for certificates that are in the "Registered" registration state.

A security server certificate can be in one of the following validity states.

- **Unknown** (validity information missing) – the certificate does not have a valid OCSP response (the OCSP response validity period is set by the X-Road governing authority) or the last OCSP response was either "unknown" (the responder doesn't know about the certificate being requested) or an error.
- **Suspended** – the last OCSP response about the certificate was "suspended".
- **Good** (valid) – the last OCSP response about the certificate was "good". Only certificates in the "good" (valid) state can be used to sign messages or establish a connection between security servers.
- **Expired** – the certificate's validity end date has passed. The certificate is not active and OCSP queries are not performed about it.
- **Revoked** – the last OCSP response about the certificate was "revoked". The certificate is not active and OCSP queries are not performed about it.
- **Disabled** – the user has marked the certificate as disabled. The certificate is not active and OCSP queries are not performed about it.

5.4. ACTIVATING AND DISABLING THE CERTIFICATES

Access rights

- For authentication certificates: Security Officer
- For signing certificates: Security Officer, Registration Officer

Disabled certificates are not used for signing messages or for establishing secure channels between security servers (authentication). If a certificate is disabled, its

status in the "OCSP response" column in the "Keys and Certificates" table is "Disabled".

To activate or disable a certificate, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. To activate a certificate, select an inactive certificate from the table and click **Activate**. To deactivate a certificate, select an active certificate from the table and click **Disable**.

5.5. CONFIGURING AND REGISTERING AN AUTHENTICATION KEY AND CERTIFICATE

A Security server can have multiple authentication keys and certificates (e.g., during authentication key change).

The process of configuring another authentication key and certificate is described in Section 3.2.

The process of registering an authentication certificate is described in Section 3.3.1.

5.6. DELETING A CERTIFICATE

An authentication certificate registered or submitted for registration in the X-Road governing authority (indicated by the "Registered" or "Registration in progress" state) must be unregistered before it can be deleted. The unregistering event sends an authentication certificate deletion request from the security server to the central server.

5.6.1. UNREGISTERING AN AUTHENTICATION CERTIFICATE

Access rights: Security Officer

To unregister an authentication certificate, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. Select an authentication certificate in the state "Registered" or "Registration in progress" and click **Unregister**.
Next, an authentication certificate deletion request is automatically sent to the X-Road central server, upon the receipt of which the associated authentication certificate is deleted from the central server. If the request was successfully sent, the message "Request sent" is displayed and the authentication certificate is moved to the "Deletion in progress" state.

A registered authentication certificate can be deleted from the central server without sending a deletion request through the security server. In this case, the security server's administrator must transmit a request containing information about the authentication certificate to be deleted to the central server's administrator. If the authentication certificate has been deleted from the central

server without a deletion request from the security server, the certificate is shown in the "Global error" state in the security server.

5.6.2. DELETING A CERTIFICATE OR A CERTIFICATE SIGNING REQUEST NOTICE

Access rights

- For authentication certificates: Security Officer
- For signing certificates: Security Officer, Registration Officer

An authentication certificate saved in the system configuration can be deleted if its state is "Saved", "Global error" or "Deletion in progress". The signing certificate and request notices can always be deleted from the system configuration.

If a certificate is stored on a hardware security token, then the deletion works on two levels:

- if the certificate is saved in the server configuration, then the deletion **deletes the certificate from server configuration**, but not from the security token;
- if the certificate is not saved in the server configuration (the background of the certificate is yellow), then the deletion deletes the certificate from the security token (assuming the token supports this operation).

To delete a certificate or a signing request notice, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. Select from the table a certificate or a certificate signing request notice and click **Delete**. Confirm the deletion by clicking **Confirm**.

5.7. DELETING A KEY

Warning: Deleting a key from the server configuration also deletes all certificates (and certificate signing request notices) associated with the key.

Access rights

- For authentication keys: Security Officer
- For signing keys: Security Officer, Registration Officer
- For keys without a role: Security Officer, Registration Officer

The deletion of keys works on two levels:

- if the key is saved in the server configuration, then the deletion **deletes the key** (and associated certificates) **from server configuration**, but not from the security token;
- if the key is not saved in the server configuration (the background of the key is yellow), then the deletion **deletes the key from the security token** (assuming the token supports this operation).

To delete a key, follow these steps.

1. On the **Management** menu, select **Keys and Certificates**.
2. Select a key and click **Delete**. Confirm the deletion of the key (and its associated certificates) by clicking **Confirm**.

6. X-ROAD SERVICES

The services are managed on two levels:

- the addition, deletion, and deactivation of services is carried out on the WSDL level;
- the service address, internal network connection method, and the service timeout values are configured at the service level. However, it is easy to extend the configuration of one service to all the other services in the same WSDL.

6.1. ADDING A WSDL

Access rights: Service Administrator

When a new WSDL file is added, the security server reads service information from it and displays the information in the table of services. The service code, title and address are read from the WSDL.

To add a WSDL, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Click **Add WSDL**, enter the WSDL address in the window that opens and click **OK**. The WSDL and the information about the services it contains are added to the table. By default, the WSDL is added in disabled state (see 6.3).

To see a list of services contained in the WSDL

- click the “+” symbol in front of the WSDL row to expand the list.

6.2. REFRESHING A WSDL

Access rights: Service Administrator

Upon refreshing, the security server reloads the WSDL file from the WSDL address to the security server and checks the service information in the reloaded file against existing services. If the composition of services in the new WSDL has changed compared to the current version, a warning is displayed and you can either continue with the refresh or cancel.

To refresh the WSDL, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select from the table a WSDL to be refreshed and click **Refresh**.

3. If the new WSDL contains changes compared to the current WSDL in the security server, a warning is displayed. To proceed with the refresh, click **Continue**.

When the WSDL is refreshed, the existing services' settings are not overwritten.

6.3. ENABLING AND DISABLING A WSDL

Access rights: Service Administrator

A disabled WSDL is displayed in the services' table in red with a "Disabled" note.

Services described by a disabled WSDL cannot be accessed by the service clients – if an attempt is made to access the service, an error message is returned, containing the information entered by the security server's administrator when the WSDL was disabled.

If a WSDL is enabled, the services described there become accessible to users. Therefore it is necessary to ensure that before enabling the WSDL, the parameters of all its services are correctly configured (see 6.6).

To **enable** a WSDL, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select a disabled WSDL from the table and click **Enable**.

To **disable** a WSDL, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. To enable a WSDL, select an enabled WSDL from the table and click **Disable**.
3. In the window that opens, enter an error message, which is shown to clients who try to access any of the services in the WSDL, and click **OK**.

6.4. CHANGING THE ADDRESS OF A WSDL

Access rights: Service Administrator

To change the WSDL address, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select from the table a WSDL whose address you wish to change and click **Edit**.
3. In the window that opens, edit the WSDL address and click **OK**. When the address is changed, the WSDL is refreshed (see section 6.2).

6.5. DELETING A WSDL

Access rights: Service Administrator

When a WSDL is deleted, all information related to the services described in the WSDL, including access rights, are deleted.

To delete a WSDL, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select from the table a WSDL to be deleted and click **Delete**.
3. Confirm the deletion by clicking **Confirm** in the window that opens.

6.6. CHANGING THE PARAMETERS OF A SERVICE

Access rights: Service Administrator

Service parameters are

- "Service URL" - the URL where requests targeted at the service are directed;
- "Timeout (s)" - the maximum duration of a request to the database, in seconds;
- "Verify TLS certificate" - toggles the verification of the certificate when a TLS connection is established.

To change service parameters, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select a service from the table and click **Edit**.
3. In the window that opens, configure the service parameters. To apply the selected parameter to all services described in the same WSDL, select the checkbox adjacent to this parameter in the **Apply to All in WSDL** column. To apply the configured parameters, click **OK**.

7. ACCESS RIGHTS

Access rights can be granted to the following access right subjects.

- **An X-Road member's subsystem.**
- **A global access rights group.** Global groups are created in the X-Road governing authority. If a group is granted an access right, it extends to all group members.
- **A local access rights group.** To simplify access rights management, each client in the security server can create local access rights groups (see section 8). If a group is granted an access right, it extends to all group members.

There are two options for managing access rights in a security server.

- Service-based access rights management – if a single service needs to be opened/closed to multiple service clients (see 7.1).
- Service client-based access rights management – if a single service client needs multiple services opened/closed (see 7.2).

7.1. CHANGING THE ACCESS RIGHTS OF A SERVICE

Access rights: Service Administrator

To change the access rights to a service, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select a service from the table and click **Access Rights**.
3. In the window that opens, the access rights table displays information about all X-Road subsystems and groups that have access to the selected service.
4. To add one or more access right subjects to the service, click **Add Subjects**. The subject search window appears. You can search among all subsystems and global groups registered in the X-Road governing authority and among the security server client's local groups. Select one or more subjects from the table and click **Add Selected to ACL**. To grant the access right to all subjects in the search results, click **Add All to ACL**.
5. To remove service access rights subjects, select the respective rows in the access rights table and click **Remove Selected**. To clear the access rights list (that is, remove all subjects), click **Remove All**.

7.2. ADDING A SERVICE CLIENT

Access rights: Service Administrator

The service client view (**Configuration** -> **Security Server Clients** -> **Service Clients**) displays all the access rights subjects of the services mediated by this security server client. In other words, if an X-Road subsystem or group has been

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

granted the access right to a service of this client, then the subject is shown in this view.

To add a service client, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**.
2. Select a client from the table and click the **Service Clients** icon, then click **Add**.
3. In the window that opens, locate and select a subject (a subsystem, or a local or global group) to which you want to grant access rights to and click **Next**.
4. Locate the service(s) whose access rights you want to grant to the selected subject. Click **Add Selected to ACL** to grant access rights to the selected services to this subject. Click **Add All to ACL** to grant access rights to all services in the filter to the subject.

The subject is added to the list of service clients, after which the service client's access rights view is displayed where the access rights can be changed.

7.3. CHANGING THE ACCESS RIGHTS OF A SERVICE CLIENT

Access rights: Service Administrator

To change the service client's access rights, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Service Clients** icon on that row.
2. In the window that opens, locate and select a subject (a subsystem, or a local or global group) whose access rights you want to change and click **Access Rights**.
3. In the window that opens, a list of services opened in the security server to the selected subject is displayed.
 - To remove access rights to a service from the service client, select one or more services from the table and click **Remove Selected**, then click **Confirm**.
 - To remove all access rights from the service client, click **Remove All** and then click **Confirm**.
 - To add access rights to a service client, start by clicking **Add Service**. In the window that opens, select the service(s) that you wish to grant to the subject (already granted services are displayed in gray) and click **Add Selected to ACL**. To add all services found by the search, click **Add All to ACL**.

Caution: If you refresh the page, all service clients that do not have access rights to any services are removed from the service clients' view.

8. LOCAL ACCESS RIGHT GROUPS

A local access rights group can be created for a security server client in order to facilitate the management of service access rights for a group of X-Road subsystems that use the same services. The access rights granted for a group apply for all the members of the group. Local groups are client-based, that is, a local group can only be used to manage the service access rights of one security server client in one security server.

8.1. ADDING A LOCAL GROUP

Access rights: Service Administrator

To create a local group for a security server client, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client and click the **Local Groups** icon on that row. In the window that opens, a list of the client's local groups is displayed.
2. To create a new group, click **Add Group**. In the window that opens, enter the code and description for the new group and click **OK**.

8.2. DISPLAYING AND CHANGING THE MEMBERS OF A LOCAL GROUP

Access rights: Service Administrator

To **view the members** of a local group, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client and click the **Local Groups** icon on that row.
2. In the window that opens, select a group whose members you want to view or change, and click **Details** to open the detail view.

To **add one or more members** to a local group, follow these steps in the group's detail view.

1. Click **Add Members**.
2. In the window that opens, locate and select the subsystems that you wish to add to the group and click **Add Selected to Group**. To add all subsystems found by the search function to the group, click **Add All to Group**.

To **remove members** from a local group, select the members to be deleted in the group's detail view and click **Remove Selected Members**. To remove all group members from the group, click **Remove All Members**.

8.3. CHANGING THE DESCRIPTION OF A LOCAL GROUP

Access rights: Service Administrator

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

To change the description of a local group, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Local Groups** icon on that row.
2. Select a group from the local groups table and click **Details**.
3. In the group detail view, click **Edit** to change the description.
4. Enter the group description and click **OK**.

8.4. DELETING A LOCAL GROUP

Access rights: Service Administrator

Warning: When a local group is deleted, all the group members' access rights, which were granted through belonging to the group, are revoked.

To delete a local group, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Local Groups** icon on that row.
2. Select a group from the local groups table and click **Details**.
3. In the group detail view, click **Delete Group** and confirm the deletion by clicking **Confirm** in the window that opens.

9. COMMUNICATION WITH THE CLIENT INFORMATION SYSTEMS

Access rights: Registration Officer, Service Administrator

A security server can use either the HTTP, HTTPS, or HTTPS NOAUTH protocol to communicate with information system servers which provide and use services.

- The HTTP protocol should be used if the information system server and the security server communicate in a private network segment where no other computers are connected to. Furthermore, the information system server must not allow interactive log-in.
- The HTTPS protocol should be used if it is not possible to provide a separate network segment for the communication between the information system server and the security server. In that case, cryptographic methods are used to protect their communication against potential eavesdropping and interception. Before HTTPS can be used, internal TLS certificates must be created for the information system server(s) and loaded to the security server.
- The HTTPS NOAUTH protocol should be used if you want the security server to skip the verification of the information system TLS certificate.

Note: If the HTTP connection method is selected, but the information system connects to the security server over HTTPS, then the connection is accepted, but the client's internal TLS certificate is not verified (same behavior as with HTTPS NOAUTH).

To set the connection method for internal network servers in the **service consumer role**, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Internal Servers** icon on that row.
2. On the **Connection Type** drop-down, select the connection method and click **Save**.

Depending on the configured connection method, the request URL for information system is **http://SECURITYSERVER/** or **https://SECURITYSERVER/**. When making the request, the address SECURITYSERVER must be replaced with the actual address of the security server.

The connection method for internal network servers in the **service provider role** is determined by the protocol in the URL. To change the connection method, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Services** icon on that row.
2. Select a service from the table and click **Edit**.

3. Change the protocol in the service URL to HTTP or HTTPS.
If the HTTPS protocol was selected, select the **Verify TLS certificate** checkbox if needed (see section 6.6). According to the service parameters, the connection with the internal network server is created using one the following protocols:
 - HTTP – the service/adaptor URL begins with “**http://...**”.
 - HTTPS – the service/adaptor URL begins with “**https://**” and the **Verify TLS certificate** checkbox is selected.
 - HTTPS NOAUTH – the service/adaptor URL begins with “**https://**” and the **Verify TLS certificate** checkbox is not selected.

To add an internal TLS certificate for a security server client (for HTTPS connections), follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Internal Servers** icon on that row.
2. To add a certificate, click **Add** in the **Internal TLS Certificates** section, select a certificate file from the local file system and click **OK**. The certificate fingerprint appears in the “Internal TLS Certificates” table.

To display the detailed information of an internal TLS certificate, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Internal Servers** icon on that row.
2. Select a certificate from the “Internal TLS Certificates” table and click **Details**.

To delete an internal TLS certificate, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Internal Servers** icon on that row.
2. Select a certificate from the “Internal TLS Certificates” table and click **Delete**.
3. Confirm the deletion by clicking **Confirm** in the window that opens.

To export the security server's internal TLS certificate, follow these steps.

1. On the **Configuration** menu, select **Security Server Clients**, select a client from the table and click the **Internal Servers** icon on that row.
2. Click **Export** and save the prompted file to the local file system.

10. SYSTEM PARAMETERS

The security server system parameters are:

- **Configuration anchor's information.** The configuration anchor contains data that is used to periodically download signed configuration from the central server and to verify the signature of the downloaded configuration.
- **Timestamping service information.** Timestamping is used to preserve the evidential value of messages exchanged over X-Road.
- **The internal TLS key and certificate.** The internal TLS certificate is used to establish a TLS connection with the security server client's information system if the "HTTPS" connection method is chosen for the client's servers.

10.1. MANAGING THE CONFIGURATION ANCHOR

Access rights

- For uploading the configuration anchor: Security Officer
- For downloading the configuration anchor: Security Officer, System Administrator

To upload the configuration anchor, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the **Configuration Anchor** section, click **Upload**.
3. Find the anchor file from the local file system and click **Upload**.
4. Ensure that the anchor file you are uploading is valid by comparing the hash value of the uploaded file with the hash value of the currently valid anchor published by the X-Road governing authority. If the hash values match, confirm the upload by clicking **Confirm**.

To download the configuration anchor, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. On the **Configuration Anchor** section, click **Download** and save the prompted file.

10.2. MANAGING THE TIMESTAMPING SERVICES

Access rights: Security Officer

To add a timestamping service, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the **Timestamping Services** section, click **Add**.
3. In the window that opens, select a service and click **OK**.

To delete a timestamping service, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the **Timestamping Services** section, select the service to be deleted and click **Delete**.

Note: If more than one time stamping service is configured, the security server will try to get a timestamp from the topmost service in the table, moving down to the next service if the try was unsuccessful.

10.3. CHANGING THE INTERNAL TLS KEY AND CERTIFICATE

Access rights: Security Officer, System Administrator

To change the security server's internal TLS key and certificate, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the **Internal TLS Certificate** section, click **Generate New TLS Key** and in the window that opens, click **Confirm**.

The security server generates a key used for communication with the client information systems, and the corresponding self-signed certificate. The security server's certificate fingerprint will also change. The security server's domain name is saved to the certificate's *Common Name* field, and the internal IP address to the *subjectAltName* extension field.

To generate a new certificate request, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the "Internal TLS Certificate" section, click **Generate Certificate Request**, input the **Distinguished Name** and save the certificate request file to the local file system.

The security server generates a certificate request using the current key and the provided **Distinguished Name**.

To import a new TLS certificate, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the "Internal TLS Certificate" section, click **Import Certificate** and point to the file to be imported.

The imported certificate must be in PEM-format to be accepted. Note that importing a new TLS certificate will restart the xroad-proxy and thus affects providing services from the security server.

To export the security server's internal TLS certificate, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the **Internal TLS Certificate** section, click **Export** and save the prompted file to the local file system.

To view the detailed information of the security server's internal TLS certificate, follow these steps.

1. On the **Configuration** menu, select **System Parameters**. The system parameters view is opened.
2. In the **Internal TLS Certificate** section, click **Certificate Details**.

11. MESSAGE LOG

The purpose of the message log is to provide 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 (Associated Signature Container [ASiC]).

Message log data is stored to the database of the security server during message exchange. According to the configuration (see 11.1), the timestamping of the signatures of the exchanged messages is either synchronous to the message exchange process or is done asynchronously using the time period set by the X-Road governing agency.

In case of synchronous timestamping, the timestamping is an integral part of the message exchange process (one timestamp is taken for the request and another for the response). If the timestamping fails, the message exchange fails as well and the security server responds with an error message.

In case of asynchronous timestamping, all the messages (maximum limit is determined in the configuration, see 11.1) stored in the message log since the last periodical timestamping event are timestamped with a single (batch) timestamp. By default, the security server uses asynchronous timestamping for better performance and availability.

The security server periodically composes signed (and timestamped) documents from the message log data and archives them in the local file system. Archive files are ZIP containers containing one or more signed documents and a special linking information file for additional integrity verification purpose.

11.1. CHANGING THE CONFIGURATION OF THE MESSAGE LOG

Configuration parameters are defined in INI files [INI], where each section contains the parameters for a particular security server component. The default message log configuration is located in the file

`/etc/xroad/conf.d/addons/message-log.ini.`

In order to override default values, create or edit the file

`etc/xroad/conf.d/local.ini.`

Create the [message-log] section (if not present) in the file. Below the start of the section, list the values of the parameters, one per line.

For example, to configure the parameters

`archive-path` and `archive-max-filesize`,

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

the following lines must be added to the configuration file:

```
[message-log]
archive-path=/my/archive/path/
archive-max-filesize=67108864
```

11.1.1. COMMON PARAMETERS

1. hash-algo-id – the hash algorithm that is used for hashing in the message log. Possible choices are SHA-256, SHA-384, SHA-512. Defaults to SHA-512.

11.1.2. TIMESTAMPING PARAMETERS

1. timestamp-immediately – if set to true, the timestamps are created synchronously with the message exchange, i.e., one timestamp is created for a request and another for a response. This is a security policy to guarantee the timestamp at the time of logging the message, but if the timestamping fails, the message exchange fails as well, and if load to the security server increases, then the load to the timestamping service increases as well. The value of this parameter defaults to false for better performance and availability. In case the value of the parameter is false then the timestamping is performed as a periodic background process (the time period is determined in the X-Road governing agency and propagated to the security servers by global configuration) and signatures stored during the time period (see parameter timestamp-records-limit) are timestamped in one batch.
2. timestamp-records-limit – maximum number of signed messages that can be timestamped in one batch. The message exchanging load (messages per minute) and the timestamping interval of the security server must be taken into account when changing the default value of this parameter. Do not modify this parameter without a good reason. Defaults to 10000.
3. acceptable-timestamp-failure-period – time period in seconds, for how long the asynchronous timestamping is allowed to fail before message exchange between security servers is stopped. Set to 0 to disable this check. Defaults to 14400.

11.1.3. ARCHIVING PARAMETERS

1. keep-records-for – time in days for which to keep timestamped and archived records in the database. Defaults to 30.
2. archive-max-filesize – maximum size for archived files in bytes. Reaching the maximum value triggers the file rotation. Defaults to 33554432 (32 MB).
3. archive-interval – time interval as Cron expression [**CRON**] for archiving timestamped records. Defaults to 0 0 0/6 1/1 * ? * (fire every 6 hours).
4. archive-path – the directory where the timestamped log records are archived. Defaults to /var/lib/xroad/.

5. `clean-interval` – time interval as Cron expression [**CRON**] for cleaning archived records from the database. Defaults to `0 0 0/12 1/1 * ? *` (fire every 12 hours).
6. `archive-transfer-command` – the command executed after the (periodic) archiving process. This enables one to configure an external script to transfer archive files automatically from the security server. Defaults to no operation.

11.2. TRANSFERRING THE ARCHIVE FILES FROM THE SECURITY SERVER

In order to save hard disk space, it is recommended to transfer archive files periodically from the security server (manually or automatically) to an external location.

Archive files (ZIP containers) are located in the directory specified by the configuration parameter `archive-path`. File names are in the format `mlog-X-Y-Z.zip`, where X is the timestamp (UTC time in the format `YYYYMMDDHHmmss`) of the first message log record, Y is the timestamp of the last message log record (records are processed in chronological order) and Z is 10 characters long alphanumeric random. An example of an archive file name is:

`mlog-20150504152559-20150504152559-a7JS05XAJC.zip`

The message log package provides a helper script `/usr/share/xroad/scripts/archive-http-transporter.sh` for transferring archive files. This script uses the HTTP/HTTPS protocol (the POST method, the form name is `file`) to transfer archive files to an archiving server.

Usage of the script:

Options:

<code>-d, --dir DIR</code>	Archive directory. Defaults to <code>'/var/lib/xroad'</code>
<code>-r, --remove</code>	Remove successfully transported files from the archive directory.
<code>-k, --key KEY</code>	Private key file name in PEM format (TLS). Defaults to <code>'/etc/xroad/ssl/internal.key'</code>
<code>-c, --cert CERT</code>	Client certificate file in PEM format (TLS). Defaults to <code>'/etc/xroad/ssl/internal.crt'</code>
<code>--cacert FILE</code>	CA certificate file to verify the peer (TLS). The file may contain multiple CA certificates. The certificate(s) must be in PEM format.
<code>-h, --help</code>	This help text.

The archive file has been successfully transferred when the archiving server returns the HTTP status code 200.

Override the configuration parameter `archive-transfer-command` (create or edit the file `etc/xroad/conf.d/local.ini`) to set up a transferring script. For example:

```
[message-log]
archive-transfer-command=/usr/share/xroad/scripts/archive-http-transporter.sh -r http://my-archiving-server/cgi-bin/upload
```

The message log package contains the CGI script `/usr/share/doc/xroad-addon-message-log/archive-server/demo-upload.pl` for a demo archiving server for the purpose of testing or development.

11.3. USING A REMOTE DATABASE

The message log database can be located outside of the security server. The following guide describes how to configure and populate a remote database schema for the message log. It is assumed that access to the database from the security server has been configured. For detailed information about the configuration of database connections, refer to [JDBC].

1. Create a database user at remote database host:

```
postgres@db_host:~$ createuser -P message_log_user
Enter password for new role: <message_log_password>
Enter it again: <message_log_password>
```

2. Create a database owned by the message log user at remote database host:

```
postgres@db_host:~$ createdb message_log_dbname -O message_log_user
-E UTF-8
```

3. Verify connectivity from security server to the remote database:

```
user@security_server:~$ psql -h db_host -U message_log_user
message_log_dbname
Password for user message_log_user: <message_log_password>
psql (9.3.9)
SSL connection (cipher: DHE-RSA-AES256-GCM-SHA384, bits: 256)
Type "help" for help.
```

```
message_log_dbname=>
```

4. Stop xroad-proxy service for reconfiguration:

```
root@security_server:~ # service xroad-proxy stop
```

5. Configure the database connection parameters to achieve encrypted connections, in /etc/xroad/db.properties:

```
messagelog.hibernate.jdbc.use_streams_for_binary = true
messagelog.hibernate.dialect =
ee.ria.xroad.common.db.CustomPostgreSQLDialect
messagelog.hibernate.connection.driver_class =
org.postgresql.Driver
messagelog.hibernate.connection.url =
jdbc:postgresql://db_host:5432/messagelog_dbname?
ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
messagelog.hibernate.connection.username = messagelog_user
messagelog.hibernate.connection.password = messagelog_password
```

6. Populate database schema by reinstalling messagelog addon package (it will start xroad-proxy service also):

```
root@security_server:~ # apt-get install --reinstall xroad-addon-
messagelog
```

12. AUDIT LOG

The security server keeps an audit log. The audit log events are generated by the user interface when the user changes the system's state or configuration. The user actions are logged regardless of whether the outcome was a success or a failure. The complete list of the audit log events is described in [SPEC-AL].

Actions that change the system state or configuration but are not carried out using the user interface are not logged (for example, X-Road software installation and upgrade, user creation and permission granting, and changing the configuration files).

An audit log record contains

- the description of the user action,
- the date and time of the event,
- the username of the user performing the action, and
- the data related to the event.

For example, registering a new client in the security server produces the following log record:

```
2015-07-03T10:21:59+03:00 my-security-server-host INFO [X-Road  
Proxy UI] 2015-07-03 10:21:59+0300 - {"event":"Register  
client","user":"admin1", "data":{"clientIdIdentifier":  
{"xRoadInstance":"EE","memberClass":"COM",  
"memberCode":"member1"},"clientStatus":"registration in progress"}}
```

The event is present in JSON [JSON] format, in order to ensure machine processability. The field event represents the description of the event, the field user represents the user name of the performer, and the field data represents data related with the event. The failed action event record contains an additional field reason for the error message. For example:

```
2015-07-03T11:55:39+03:00 my-security-server-host INFO [X-Road  
Proxy UI] 2015-07-03 11:55:39+0300 - {"event":"Log in to token  
failed","user":"admin1", "reason":"PIN incorrect","data":  
{"tokenId":"0","tokenSerialNumber":null,  
"tokenFriendlyName":"softToken-0"}}
```

By default, audit log is located in the file

```
/var/log/xroad/audit.log
```

12.1. CHANGING THE CONFIGURATION OF THE AUDIT LOG

The X-Road software writes the audit log to the *syslog* (*rsyslog*) using UDP interface (default port is 514). Corresponding configuration is located in the file

```
/etc/rsyslog.d/90-udp.conf
```

The audit log records are written with level INFO and facility LOCAL0. By default, log records of that level and facility are saved to the X-Road audit log file

```
/var/log/xroad/audit.log
```

The default behavior can be changed by editing the *rsyslog* configuration file

```
/etc/rsyslog.d/40-xroad.conf
```

Restart the *rsyslog* service to apply the changes made to the configuration file

```
restart rsyslog
```

The audit log is rotated monthly by *logrotate*. To configure the audit log rotation, edit the *logrotate* configuration file

```
/etc/logrotate.d/xroad-proxy
```

12.2. ARCHIVING THE AUDIT LOG

In order to save hard disk space and avoid loss of the audit log records during security server crash, it is recommended to archive the audit log files periodically to an external storage or a log server.

The X-Road software does not offer special tools for archiving the audit log. The *rsyslog* can be configured to redirect the audit log to an external location.

13. BACK UP AND RESTORE

13.1. BACK UP AND RESTORE IN THE USER INTERFACE

Access rights: System Administrator

The backup and restore view can be accessed from the **Management** menu by selecting **Back Up and Restore**.

To **back up configuration**, follow these steps.

1. Click **Back Up Configuration**.
2. A window opens displaying the output of the backup script; click **OK** to close it. The configuration backup file appears in the list of configuration backup files.
3. To save the configuration backup file to the local file system, click **Download** on the configuration file's row and save the prompted file.

To **restore configuration**, follow these steps.

1. Click **Restore** on the appropriate row in the list of configuration backup files and click **Confirm**.
2. A window opens displaying the output of the restore script; click **OK** to close it.

To **delete a configuration backup file**, click **Delete** on the appropriate row in the configuration backup file list and then click **Confirm**.

To **upload a configuration backup file** from the local file system to the security server, click **Upload Backup File**, select a file and click **OK**. The uploaded configuration file appears in the list of configuration files.

13.2. RESTORE FROM THE COMMAND LINE

To restore configuration from the command line, the following data must be available:

- The X-Road ID of the security server

It is expected that the restore command is run by the xroad user.

In order to restore configuration, the following command should be used:

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh \  
-s <security server ID> -f <path + filename>
```

For example (all on one line):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh \  
-s AA/GOV/TS10WNER/TS1 \  
-f /var/lib/xroad/backup/conf_backup_20140703-110438.tar
```

If it is absolutely necessary to restore the system from a backup made on a different security server, the forced mode of the restore command can be used with the -F option. For example (all on one line):

```
/usr/share/xroad/scripts/restore_xroad_proxy_configuration.sh \  
-F -f /var/lib/xroad/backup/conf_backup_20140703-110438.tar
```


14. DIAGNOSTICS

14.1. EXAMINE SECURITY SERVER SERVICES STATUS INFORMATION

Access rights: System Administrator

Open the **Management** menu and select **Diagnostics**.

On this page you can examine the statuses of the following services.

Service	Status	Message	Previous Update	Next Update
Global configuration	Green/yellow/red	Status message	The time of the global configuration client's last run	The estimated time of the global configuration client's next run
Timestamping	Green/yellow/red	Status message	The time of the last timestamping operation	Not used

To refresh the service statuses click again the **Diagnostics** item on the **Management** menu.

15. LOGS AND SYSTEM SERVICES

To read logs, a user must have root user's rights or belong to the xroad and/or adm system group.

15.1. SYSTEM SERVICES

The most important system services of a security server are as follows.

Service	Purpose	Log
xroad-confclient	Client process for the global configuration distributor	/var/log/xroad/configuration_client.log
xroad-jetty	Application server running the user interface	/var/log/xroad/jetty/
xroad-proxy	Message exchanger	/var/log/xroad/proxy.log
xroad-signer	Manager process for key settings	/var/log/xroad/signer.log
nginx	Web server that exchanges the services of the user interface's application server and the message exchanger	/var/log/nginx/

System services are managed through the *upstart* facility.

To start a service, issue the following command as a root user:

```
service <service> start
```

To stop a service, enter:

```
service <service> stop
```

15.2. LOGGING CONFIGURATION

For logging, the **Logback** system is used. Logback configuration files are stored in the directory `/etc/xroad/conf.d/`.

Default settings for logging are the following:

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>

- logging level: INFO;
- rolling policy: whenever the file size reaches 100 MB.

15.3. FAULT DETAIL UUID

In case a security server encounters an error condition during the message exchange, the security server returns a SOAP Fault message [PR-MESS] containing a UUID (a universally unique identifier, e.g. 1328e974-4fe5-412c-a4c4-f1ac36f20b14) as the fault detail to the service client's information system. The UUID can be used to find the details of the occurred error from the xroad-proxy log.