X-ROAD 5

SECURITY SERVER USER'S GUIDE

5.05

VERSION HISTORY

DATE	VERSION	DESCRIPTION
28 Oct 2010	5.0	Initial version.
2 June 2011	5.01	Numerous amendments.
13 Aug 2012	5.02	Correction to the procedure “Loading the CA key”. Proofreading.
5 Oct 2012	5.03	Changed the package repository address.
30 Oct 2012	5.04	New connection method HTTPS NOAUTH for information systems / adapter servers. Connection method can now be selected individually for each server.
June 2015	5.05	Updated log archive and setting adapter server parameters.. Section for referring to other documents added. Addition for making monitoring system key at configuration recovery. Automatic configuration backup added. Restrictions to short database names specified. Security server transferred to operation system Ubuntu 14.04 LTS (64 bit). Reboot needed after installation of X-Road packs.

CONTENTS

1 INTRODUCTION

1.1 TARGET AUDIENCE

The document assumes that the reader has at least basic knowledge of networking and Linux server management.

1.2 REFERENCESA

a. Cybernetica AS. Requirements to information systems and adapter servers 9.6. (13.02.2015)
b. Cybernetica AS. X-Road 5.0. Specification of new monitoring system 0.11. (10.10.2012)
c. Cybernetica AS. User manual for query log hashing utility of X-Road security server 0.4 (10.03.2010)

1.2 X-ROAD SECURITY SERVER

The main purpose of a security server is to exchange, or broker, queries (between an organization and a database) in a way that preserves their evidentiary value. This guide describes the management and administration of the security server in an organization joined with the X-Road system.

The following scheme depicts the main components of X-Road.

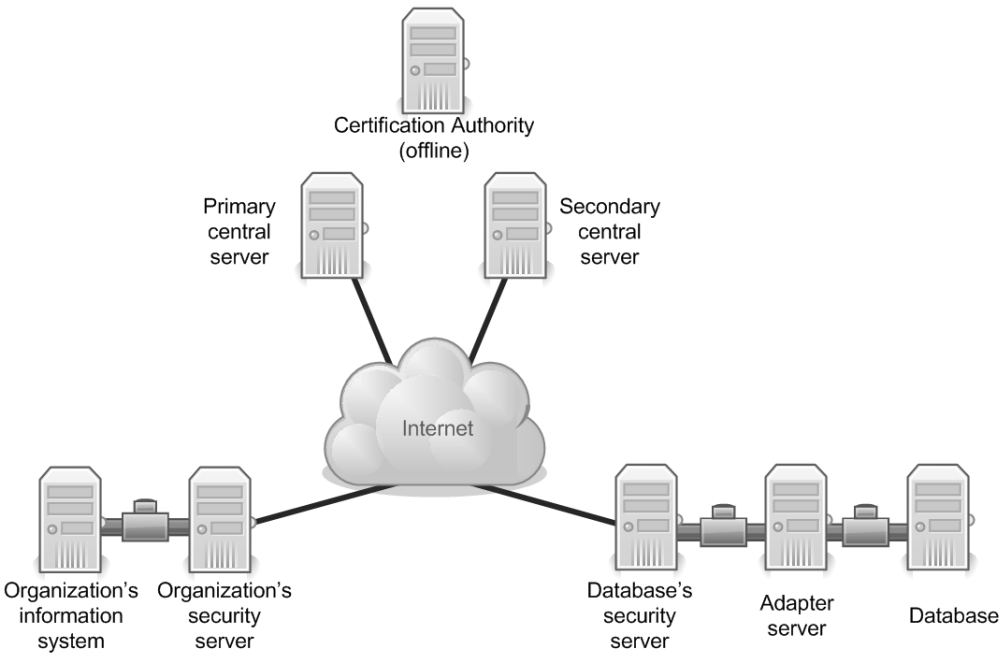


Figure 1. Main components of X-Road

Security server is connected to public Internet from one side and to an information system or adapter server located in an internal network of an institution (converting queries between database and security server) from the other side. The security server can be considered a

specialized application level firewall supporting SOAP protocol; therefore, the security server could be installed in parallel to the company firewall mediating other protocols.

A security server's main function is to ensure the security of data exchanged between an organization's information system and an adapter server.

- Data exchanged over the Internet is protected with digital signatures, and encrypted.
- To prove a case where an organization has misused data or a database has issued false data, queries are stored in a cryptographically secure log that allows to prove their occurrence any time later.
- The database's security server enforces access control on incoming queries, thus ensuring that data can be accessed only by those organizations whose databases have a valid service contract.

To ensure the availability of the system, all security servers can be doubled. One organization can use multiple, clustered security servers to perform queries. If a database uses several security servers to serve the same adapter, the queries are automatically distributed between the security servers. Should one server malfunctions, queries are automatically redirected to working security servers.

Security servers use the services of a central server, which provides name resolution and receives periodically query log hashes, thus creating a verifiable audit trail of queries.

The main duty of the security server’s administrator is to install, configure, and maintain the server. In addition, the administrator is authorized to take action during an emergency; for example, if the system is under attack and the integrity or confidentiality of data is at risk, the administrator is authorized to disconnect their security servers from the public network.

The security server's administrator must have a trained replacement who can perform all management duties. For important national databases or registries, it is essential to have two system administrators.

1.3 NEW IN VERSION 5.0

Starting from version 5.0, the security server's user interface is Web-based.

Removed functionality:

- Configuring network settings
- Stopping and restarting the server
- Removable media (CD, memory stick) support for saving and loading data
- Support for the XML-RPC protocol (from now, only SOAP is used)
- Logging queries to PostgreSQL database
- Secure mail exchange over X-Road
- The custom patching and counterpatching system
- UPS configuration functionality (it is recommended to use the "nut", or Network UPS Tools, package)

Changed functionality:

- It is assumed that the security server has one network interface by default.
- When restarting the security server, a master password, which protects all the security server's private keys, has to be entered on server console.
- Importing and exporting data is only performed through uploading and downloading files.
- Security server updates are distributed as Debian/Ubuntu packages.
- Aggregate database administration is added to database menu.

The rest of the functionality follows the old user interface as closely as possible.

2 INSTALLATION AND CONFIGURATION

2.1 PREPARATIONS

From version 5.42, the security server operates with operation system Ubuntu Server 14.04 Long-Term Support (LTS); only 64 bit platform is supported. The security server is supplied in .deb packages available from the official X-Road repository at the address http://x-road.ee.

The security server can be installed on normal as well as virtualized hardware (the server has been tested with VMWare Server and Oracle VirtualBox).

To install the security server, you will need the following information:

- The IP address of the primary central server
- The IP addresses of secondary central servers (if any)
- The DNS key fingerprint (provided by the central server's administrator)
- The CA certificate fingerprint (also provided by the central server's administrator)

This guide assumes that the security server is installed to a server with one network interface card (NIC).

- If two NICs are used, they are to be configured so that one (the external interface) connects the security server to public Internet, and the other (the internal interface) connects the server to an information system or adapter server in a local area network.
- If one NIC is used, the document's references to external and internal interfaces should be understood as pertaining to the same NIC.

Furthermore, it is advisable to read ISA FAQ at https://www.ria.ee/x-tee-keskkondade-tehnilised-parameetrid/, which includes of the test, development and product environment server addresses, authenticity codes etc.

2.2 REQUIREMENTS TO SECURITY SERVER HARDWARE

Recommended hardware parameters:

- The server in general shall be supported by Ubuntu 14.04 (motherboard, processor, network cards, storage system, graphics card);
- 64-bit Intel, AMD or compatible dual-core processor;
- 2 GB RAM;
- 100 Mbps network card;
- 1 available USB port for a memory stick.

2.3 CONFIGURING FIREWALL FOR SECURITY SERVER

Typically, the security server must be installed behind an organization's firewall, in which case the following ports must be opened.

Ports for incoming services:

- TCP 5555 – SSL/TLS data exchange between security servers

Ports for outgoing services:

- TCP 25 – SMTP, sending e-mails (including error messages) to the Internet
- TCP 37 – UNIX *time* protocol for the diagnostics subsystem;
- TCP and UDP 53 – Name server services;
- TCP 80 – HTTP, loading central server keys;
- UDP 123 – NTP, security server clock synchronization;
- TCP 5555 – SSL/TLS data exchange between security servers
- TCP 5556 – Security server query hash logging protocol;
- UDP 6666 – Data exchange with monitoring stations (new SKIP/ESP protocol in use from X-Road version 5.0)

2.4 SECURITY SERVER DOWNLOADING AND INSTALLATION

2.4.1 Downloading

To install the server, first add the address of the X-Road repository to the *apt-get* configuration file (/etc/sources.list). To use the repository, edit the file /etc/apt/sources.listas root and add the following line:

```
deb http://x-road.ee/packages trusty main
```

Then issue the commands:

```
sudo apt-get update
sudo apt-get install xtee-keyring
sudo apt-get update
sudo apt-get install xtee-proxy
sudo reboot
```

Because the X-Road packages are signed, the *xtee-keyring* package becomes necessary to trust the signing key, which later enables to verify the authenticity of *xtee-** packages and install them without warnings.

The address with the necessary repository key is https://www.ria.ee/x-tee-tarkvara/.

During the installation, you will be asked to set the master password for protecting the private keys.

Also during the installation, a default user for the Web interface is created:

User:**webadmin**
Password:*(set during the installation)*

Web users can later be added and modified from the command line (see section 11.1).

Restarting the security server after installation of X-Road packages is necessary for the fulfilment of the name solution configuration file resolv.conf.

Until you have configured keys and certificates, some of the security server's menus are disabled. The menus will become available after the DNS key and the CA key fingerprints have been entered.

After installation, the Web interface is available at **https://your-server-name:3000/**

2.4.2 Master password

Each time the security server is restarted, a master password, which protects the server's private keys, needs to be entered. This is indicated by the following prompt:

Enter security server's master password (attempt 1 of 3)

While the password is entered, nothing is displayed on screen. If the correct password is not entered in three attempts, the security server continues booting, but won't provide any services until the correct master password is given, either after another restart or on the Web interface. **The above means that a restart of the security server requires the physical presence of the system administrator.**

To change the master password, enter on command line:

```
sudo /usr/xtee/bin/setpwd
```

Also note that the master password is saved with the configuration, so when you restore the configuration, you'll need to enter the correct password (unless it is the same as the one currently in use).

2.5 SETTING CENTRAL SERVERS

In its operation, security server uses the central server, which provides domain name resolution and where the security server sends query log hashes. While there may be several central servers (one primary server and many secondary ones), they are considered as equal in the security server.

To add central servers:

1. On the **Configuration** menu, click **Servers**, then click **Central servers**.
2. Click **Add**.
3. Enter the primary central server's IP address and click **Save**.
4. Repeat the above steps to add secondary central server(s).

2.6 LOADING THE DNS KEY

Cryptography with a public key is used to ensure the integrity of data distributed through the name service of the central server. The central server signs the data with its private key, while a security server verifies it with the central server's public key (which is loaded from the central server). To avoid loading the wrong keys, the central server's administrator provides the security server's administrator with the DNS key fingerprint (authenticity code) that must be entered in the security server.

To load the DNS key:

1. On the **Configuration** menu, click **Keys and certificates**, then click **DNS keys**.
2. Click **Add new**.
3. Enter the key fingerprint received from the central server's administrator (in the form XX:XX:XX:...) and the primary central server's IP address, then click **Save**. On success, the fingerprint appears in the list with the status "Current". *(In subsequent loadings, when a valid key already exists, the new key remains in the "New" state until activation.)*

2.7 LOADING THE CERTIFICATION AUTHORITY KEY

The communication between security servers is encrypted with public key cryptography methods. For easier distribution of keys, certificates are issued by the X-Road certification authority (CA) installed at the central server. To verify such certificates, the CA's self-signed certificate must be loaded in every security server.

As the certificate is loaded from the central server over DNS, the name service must be set up correctly. To avoid loading the wrong keys, the central server provides the security server's administrator with the CA key fingerprint (authenticity code).

To load the CA certificate:

1. On the **Configuration** menu, click **Keys and certificates**, then click **CA certificates**.
2. Click **Add new**.
3. Enter the key fingerprint received from the central server's administrator (in the form XX:XX:XX...)
4. Click **OK**. On success, the fingerprint appears in the list with the status "Valid".

If loading the certificate fails with the error message "Empty answer from dns server" then the CA certificate is not yet loaded in the CA. Report the issue to the central server's administrator.

2.8 CREATING REVERSE RECORDS FOR IP ADDRESSES

Attention: This section may only apply to servers registered in Estonia.

For security servers to send mail to the Internet, every server is assigned a name according to its public IP address. (In earlier X-Road versions, such host name was generated automatically in the domain *xtee.riik.ee*, but no longer as of version 5.0.)

In addition, correct reverse conversion of IP address in DNS shall be generated for the security server in the network (or PTR record). The record can be created by the security server's administrator or their Internet service provider.

2.9 CONFIGURING SECURITY SERVER FOR MAIL EXCHANGE

The security server uses Postfix as its mail transport agent. To send e-mail from the security server, the server needs to have a name that recipients can look up from DNS. Thus, the server's name must resolve in DNS and the server's IP address must resolve to the name in DNS.

When installing Postfix, choose between one of the following host types.

- Choose "Internet host" if the security server is connected directly to the Internet;
- Choose "Internet host with smarthost" if outgoing mail has to be sent through a specific SMTP server;
- Choose "Local only" if you don't want to send mail out.

If Postfix was already configured in another mode, enter the following command for reconfiguration:

```
sudodpkg-reconfigure postfix
```

If Postfix is configured to send mail out, it will automatically start listening for incoming connections on TCP port 25, which is not permitted for security reasons. To deny incoming connections, enter the following commands after the initial (and every subsequent) configurations:

```
sudopostconf -e inet_interfaces=loopback-only
sudo postfix stop
sudo postfix start
```

3 SECURITY SERVER HARDENING

3.1 INTRODUCTION

Earlier security server versions were distributed on a CD, complete with an operating system pre-configured for maximum security. Starting from version 5.0, the security server is distributed as packages, so the responsibility for configuring the server in a correct and secure manner now lies on the server's administrator.

Disclaimer: The following recommendations are neither complete nor final.

3.2 GENERAL REQUIREMENTS

3.2.1 Miscellaneous

- To avoid situations where an attack causes a daemon to generate large log files, fulfilling the disk and rendering the system unusable, move /var/log to a separate partition.
- Write down the passwords of *root* and, if necessary, all other system users, GRUB (boot loader), and BIOS and store the paper in a safe.

3.2.2 Requirements for network configuration

- In /etc/network/interfaces, assign a static IP address to the security server.
- In /etc/resolv.conf, set the DNS server address to 127.0.0.1 and the domain to xtee.riik.ee.
- In /etc/hosts, specify the security server hostname and IP address.

3.2.3 Enforcing strong passwords

Enter on command line:

```
sudo apt-get install libpam-cracklib
```

The settings can be changed from */etc/pam.d/common-password*. By default, *libpam* enforces passwords that are at least 8 symbols in length (minlen=8) and requires that old and new passwords must differ by 3 symbols (difok=3).

3.2.4 Grub and BIOS password

If other persons besides the system administrator can access the security server, a password must be set for GRUB (the boot loader). This way, the system can still be rebooted, but a password will be required to add non-default boot options. In this case, you must also set the BIOS password and allow booting only from the hard disk.

3.2.5 Apticron

Install the "apticron" package to receive e-mail notifications about available security updates for the current server.

Enter on command line:

```
sudo apt-get install apticron
```

By default, notifications are also sent to *root*. To modify the setting, enter:

```
sudodpkg-reconfigure apticron
```

3.2.6 Configuring SSH

To configure SSH, edit the file */etc/sshd_config*.

(1) DISALLOW ROOT LOGINS

Replace the line "PermitRootLogin yes" with "PermitRootLogin no".

Attention: If root access is needed for backup or other purposes, use the directive "PermitRootLogin forced-commands-only".

(2) ALLOW ONLY SSH VERSION 2

The configuration file must contain the line "Protocol 2"

(3) ALLOW SSH ACCESS ONLY TO AUTHORIZED USERS

1. Create the "sshusers" group, containing only the users who need SSH access.
2. Add "AllowGroupssshusers" to the SSH configuration file.
3. Add the "sshusers" section to */etc/group*, containing a list of authorized users.

(4) MOVE SSH TO TO ANOTHER PORT

By default, SSH listens on port 22. To avoid certain automated attacks, move SSH to a higher port number, such as 10022.

3.2.7 Binary files with *suid* and *sgid* bits

To find the files, enter as a root user:

```
sudo find / -perm 4000 -o -perm 2000
```

To remove the suid/sgid bit, enter:

```
sudochmod -s <filename>
```

Attention: Consider the removal of each file separately. To avoid resetting the *suid* bit when the package is updated, remove the bit permanently using the *deb-statoverride* command. For example, if the utility "at" is not needed, it can be removed as follows:

```
sudodpkg-statoverride --add root root 755 /usr/bin/at
sudochownroot:root /usr/bin/at
sudochmod 755 /usr/bin/at
```

3.2.8 Root login notifications

Configure the system to send an e-mail every time someone logs in as root. Edit the file /root/.bashrc (if the Bash shell is used) and add the following line:

```
echo -e "List of users logged to `hostname` on (`date`)\n`who`" | mail -s "Root login on `date`" username@example.com
```

3.2.9 History file

When the security server packages are installed, the append-only attribute is automatically set to *.bash_history,* allowing opening of the file only for addition of lines.

3.2.10 Configuring ports

To list all listening TCP and UDP ports, enter on command line:

```
sudolsof -i -n | egrep 'COMMAND|LISTEN|TCP|UDP'
```

In order to close ports, remove the package providing the network service corresponding to the port number or ban listening in the network by another method. However, the following ports, which are necessary for the operation of the security server, must not be closed.

- Database security server (xtee-producerproxy): TCP 5555
- Information system's Apache: TCP 80 or 443
- Information system's or database's Web interface: TCP 3000
- SSH: as configured above
- ntpd: UDP *:123
- named: *localhost*, own port
- postfix: *localhost*, own port

3.3 AUTOMATIC SECURITY CONFIGURATION

Upon installing the security server package, certain security settings are automatically applied to the system. For this, a new /etc/systctl.conf file will be installed that applies stricter security settings that Ubuntu sets by default, including turning off IPv6 (except on the loopback interface, where it is necessary for *ssh -X* to work).

4 ADDING ORGANIZATIONS

Before the security server can be actually used, the parameters pertaining to the organization's information system or database must be set, and the security server must be certified in the X-Road Central Agency. The instructions are given below.

4.1 CONFIGURING LOCAL NETWORK SERVERS

If you are configuring an organization's information system (that is, the organization will use data, rather than provide it), follow the instructions on section 4.1.1.

If you are configuring a database's information system (that is, the organization will provide data to other organizations), see sections 4.1.2 and 4.3.

4.1.1 Configuring information system server for HTTPS

The security server can communicate with an information system (IS) server over HTTP (the default), HTTPS or HTTPS NOAUTH. From security server version 5.18, the connection method can be selected individually for each server.

- Use HTTP if the IS server and the security server communicate in a network segment where no other computers are connected to. Also, the IS server must not allow interactive login. **If you wish to use HTTP, continue at section 4.2.**
- Use HTTPS if a separate network segment for the IS server and security server cannot be assigned. In such case, the communication will be encrypted. To use HTTPS, certificates must be created for the IS server and loaded in the security server.
- Use HTTPS NOAUTH if the client certificate (e.g., that of the information system or adapter server) should not be verified. If this method is selected, the certificate fingerprint will not be displayed and also the certificate loading button is disabled.
  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 certificate is not verified (i.e., the behavior is the same as is in the case of HTTPS NOAUTH).

Load the IS server certificate:

1. On the **Configuration** menu, click **Servers**, then click **Information system servers**.
2. Select an organization, from the **Connection type** drop-down list select **HTTPS**, and then click **Load**.
3. Click **Browse** and load the IS server certificate from the disk. The file must be in the DER or PEM format and with the *.der* or *.pem* extension, respectively.
4. Click **OK**. On success, the certificate's fingerprint is displayed in the list of the organization's certificates.

Generate the key used for local network communication:

1. On the same page, click **Generate new key**.
2. Enter the security server's internal network interface IP address and click **OK**. The security server will generate a key for the communication with the IS server and the

adapter server, and the respective self-signed certificate. The security server's certificate fingerprint will also change. The entered domain name is stored in the field *Common Name* of the certificate and the IP address in the extension field *subjectAltName* of the certificate;

3. Click **Export certificate** and save the file to disk.
4. Click **Save** to apply the changes.
5. Transport the exported certificate to the IS server and continue certifying the organization as instructed in 4.2.

4.1.2 Configuring adapter server for HTTPS

For a database to share its data over X-Road, it must be equipped with an adapter server, which receives SOAP queries from the security server and translates them to the database's native language (such as SQL). An adapter server can be either a stand-alone application or a software module built in the database.

The database's security server can communicate with an adapter server over HTTP, HTTPS or HTTPS NOAUTH. From security server version 5.18, the connection method can be selected individually for each server.

- Use HTTP if the adapter server and the security server communicate in a network segment where no other computers are connected to. Also, the adapter server must not allow interactive login. **If you are going to use HTTP, continue at section 4.2.**
- Use HTTPS if a separate network segment for the adapter server and security server cannot be assigned. In such case, the communication is encrypted. To use HTTPS, certificates must be created for the adapter server and loaded in the security server.
- Use HTTPS NOAUTH if the client certificate (e.g., that of the information system or adapter server) should not be verified. If this method is selected, the certificate fingerprint will not be displayed and also the certificate loading button is disabled.
  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 certificate is not verified (i.e., the behavior is the same as is in the case of HTTPS NOAUTH).

To load the adapter server certificate:

1. On the **Configuration** menu, click **Servers**, then click **Adapter servers**.
2. Select an adapter server, from the **Connection type** drop-down list select **HTTPS**,and then click **Load**.
3. Click **Browse** and load the adapter server certificate from the disk. The file must be in the DER or PEM format and with the *.der* or *.pem* extension, respectively.
4. Click **OK**. On success, the certificate's fingerprint is displayed in the list of the organization's certificates.

Generate the local network key (if not yet generated):

1. Click **Generate new key**. The security server will generate a new key for communicating with the adapter server and information system servers and a respective self-signed certificate, and display the certificate's fingerprint.
2. Click **Export certificate** and save the file to disk
3. Click **Save** to apply the changes.
4. Transport the exported certificate to the adapter server and continue certifying the organization as instructed in 4.2.

4.2 CERTIFYING AN ORGANIZATION

The confidentiality, integrity, and authenticity of messages exchanged between security servers is ensured by means of message encryption. To simplify key change, the public keys of all security servers are registered in the X-Road central agency where certificates are issued to the keys.

Before an organization can use a security server, a key must be generated in the security server and a certificate received from the X-Road central agency. Certificates are distributed over central DNS.

4.2.1 Creating certificate request and key for organization's security server

Follow these steps.

1. On the **Configuration** menu, click **Organizations**.
2. Click **Add**.
3. Fill in the fields *Organization name* and *Registry code* (the registry code can only contain Latin characters, numbers, dashes and periods*; may not start with a period or a dash), then click **Save**. The new organization will be displayed on the list.
4. Click **Save certificate request**, then save the file to disk
5. Transport the certificate request to central server's administrator, with the following information:
    - The organization's official name;
    - The organization's registry code;
    - The organization's system administrator e-mail address where error notifications will be sent;
    - The security server's IP address.

ATTENTION

* – As of version 5.0, a period can be used in organization name. The objective is to enable creation of the hierarchy of sub-organizations. Although, in the context of X-Road, these are independent organizations, it enables structuring their name space, e.g. by registering organization names including the commercial registry code and an extension. **NB!** Sub-organizations can be generated from the security server version 5.19 and account shall be taken that the security servers older than 5.0 cannot see such organizations.

4.2.2 Using organization's security server certificate

After the central server's administrator has issued a certificate to an organization and entered the certificate in the DNS database, the security server can use the new certificate. Follow these steps.

1. On the **Configuration** menu, click **Organizations**
2. Select organization and click **Manage keys**
3. On the page that appears, click **Load certificates**. On success, the new certificate's fingerprint will be displayed in the current key group.
4. Click **Save** to use (activate) the certificate.

If the certificate fingerprint does not appear or the message "Empty answer from DNS server" is displayed, the reason might be one of the following.

- The certificate has not been issued yet.
- The certificate has been issued, but the updated certificate database has not imported from the CA to the central server.
- The certificate has been issued and published in the central server through DNS, but the security server's DNS cache has not been updated (an update takes place every 4-6 hours). In this case, click **Configuration** and then click **Reconfigure all** to restart named-demon and to empty the local DNS cache.

4.2.3 Adding and certifying new database

To create a certificate request for a database or registry:

1. On the **Configuration** menu, click **Databases/Registries**
2. Click **Add database**
3. Fill in the fields *Database name* and *Registry code* (the registry code can contain only Latin characters, numbers, dashes and periods*; may not start with a number, a period or a dash). In the field Registry code, enter:
    a. Short name of database, if the database is registered in the administration system for the state information system (RIHA)
    b. Registry code of database, if the database is not registered in RIHA.
4. Click **Save**. The new database will be displayed on the list.
5. Click **Save certificate request**, then save the certificate to disk
6. Transport the certificate request, and the following information, to central server's administrator:
    - The database's/registry's official name;
    - The database's/registry's short name or registry code;
    - The database's system administrator e-mail address where error notifications will be sent;
    - The security server's IP address.

ATTENTION

* – As of version 5.0, a period can be used in the name of a database. The objective is to enable creation of the hierarchy of subunits. Although, in the context of X-Road, these are independent databases, it enables structuring their name space, e.g. creating names including short name of a database and an extension. **NB! Subunits can be created only when all X-Road security servers have been updated to version 5.0, because relevant backward compatibility with old servers is lacking.**

4.2.4 Using database's security server certificate

After the central server's administrator has issued a certificate to the database/registry and entered it in the DNS database, the new certificate can be used in the security server. Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**
2. Select a database and click **Manage keys**
3. Click **Load certificates**. On success, the security server's certificate fingerprint will be displayed in the valid key group.
4. Click **Save** to use (activate) the certificate. After completing this step, it should be possible to make queries through the security server.

If the certificate fingerprint does not appear or the message "Empty answer from DNS server" is displayed, the reason might be one of the following.

- Central server administrator has not issued the certificate and has not copied it into the name service server. In this case, wait until the certificate appears in DNS database.
- The certificate has been issued and published in the central server through DNS, but the security server's DNS cache has not been updated (an update takes place every 4-6 hours). In this case, click **Configuration** and then click **Reconfigure all** to empty the local DNS cache.

4.3 SETTING ADAPTER SERVER PARAMETERS

An adapter server brokers queries between a database / registry and a security server. Information flows between the database and the adapter server according to database-specific protocol; task of the adapter server is to interpret and mediate it to the security server in standard SOAP format. An adapter server can be either a stand-alone application or a software module built in the database.

If the security server in question serves a database, its adapter server parameters must be set. Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Adapter server parameters**.
3. Fill in the fields as follows.

- **IP address** – The adapter server's IP address.
- **Port** – The port number where the adapter server receives HTTP or HTTPS queries (by default, it is 80 for HTTP and 443 for HTTPS). Attention: If you choose HTTP, make sure that HTTP is also set in the general adapter server settings page (**Configuration**>**Servers**>**Adapter servers**).
- **URI** – The directory and filename part of the adapter server's URI. For example, if the adapter server's URL is *http://server/directory/file* then enter */directory/file* in the URI field.
- **Schema URI** – The file containing the description of methods implemented in the adapter server. For instance, if the service descriptions' URL is *http://server/directory/database.wdsl* then enter */directory/database.wsdl* in the field. Also see the comment [*]
- **Maximum time to process one incoming query (sec)** – Self-descriptive, but note: choose a time value that exceeds the total time spent for processing the query in the adapter server and exchanging the query between security servers. ***If the query or the response is a SOAP message with attachments, the time limits are switched to another mode***, wherein this value specifies the maximum time allowed to elapse during the data exchange. Also see the comment [**].
- **Heartbeat query interval (sec)** – The interval between test queries that check whether the database is operational. Enter *0* (zero) to switch off the check.
- Translate organization name (0/1) – whether to translate the name of the organization after receiving the query in case of incoming queries after checking access rights by forwarding only the name of sub-organization to the adapter server – the part of organization name following the last period. In this case, also the response received from the adapter server shall be translated. By default 0 (not translated), in case of 1 translated.

4. Click **Save**.

Notes:

[*] As of version 5.0, the security server supports download of XForms files describing the services. XForms are searched in the same directory with WSDL-schema, i.e. file name in the field "Scheme URI" is replaced automatically with XForms file name upon search. Thus, the query form shall be in the following style: *http://server/cgi-bin/uriproxy?producer=database&filename=service.version.xhtml*.

[**] The switching takes place only after the first part of a query with attachments (a SOAP message) has arrived in the security server. It means that for a normal query and a response with attachments, the adapter server must send to the security server at least the first part of the message with attachments during the time period specified herein. A similar restriction is on the organization's security server side, where it might be necessary to extend the time limit for processing large queries.

4.4 SETTING ACCESS RIGHTS FOR ORGANIZATIONS AND GROUPS

4.4.1 Introduction

To use a database's security server, a list of queries supported by the adapter server must be loaded in the security server, and access rights must be set.

In X-Road, access to data is controlled by the owners of the data. Access rights control is performed at the database's security server, and the rights to perform one query or another are granted to organizations or organization groups as a whole. It is up to the organization to grant access rights to its individual employees.

Attention: Valid access rights control within the organization's information system is a prerequisite for joining X-Road.

The organization grouping functionality provides for aneasier security server management. As with organizations, organization groups can be granted various access rights. Note that organization groups are created in the certification authority and cannot be changed in the security server.

Access rights can be managed in two modes:

- The **Show by groups** mode (default) allows to assign one or more queries to a single organization or group. For clarity, the section covers only this mode.
- The **Show by queries** mode allows specifying one or more organizations/groups that can perform one particular query.

4.4.2 Setting access rights

Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Access rights***(requires a configured adapter server; otherwise, the button is disabled)*. Two columns are displayed: one contains a list of groups/organizations (emtpy, if it has not been loaded from the adapter server), the other contains a list of queries supported by the adapter server.
3. Click **Add** to select organizations for granting access rights. You can choose from the list containing all subjects registered in the X-Road central agency. By default, only groups are displayed; to also display organizations, select the **Show organizations** checkbox.
4. Click all applicable groups/organizations, and then click **OK**. The selected subjects will be displayed in the list (groups in blue, organizations in black)
5. Click **Refresh** to load a list of supported adapter server queries to the security server.
6. Grant access rights for organizations/groups: on the leftmost list, select organizations or groups, and on the rightmost list, select the checkboxes for queries that the subject is allowed to perform. If query encryption is also needed, see instructions in chapter 7.5.
7. Click **OK** to apply the changes.

4.4.3 Troubleshooting

If the organization/group name is displayed in brackets, it has been removed from the certification authority, in which case it is recommended to remove the organization/group also from the security server. However, if all organizations and groups are displayed in brackets, it probably indicates a malfunction in the communication between the security server and central server.

If loading the queries fails, the reason is usually either invalid adapter server parameters or invalid adapter server configuration. For example, the error message "Invalid content type: text/html" could mean one of the following.

- The adapter server URI is invalid, causing the adapter server to respond with an HTML "404 Not Found" error message. Make sure that correct parameters have been set on the **Configuration**>**Servers**>**Adapter servers** page.
- There is a problem with adapter server configuration or implementation, causing the SOAP response type to be *text/html* instead of *text/xml*. In this case, fix the problem in the adapter server and refresh the queries.

5 MANAGING THE DATABASE'S SECURITY SERVER

5.1 INTRODUCTION

For a database to share its data over X-Road, it must be equipped with an adapter server. The adapter server receives SOAP queries from the security server and translates them to the database's native language (such as SQL). An adapter server can be either a stand-alone application or a software module built in the database.

The database's security server can communicate with an adapter server over HTTP or HTTPS.

- Use HTTP if the adapter server and the security server communicate in a network segment where no other computers are connected to. Also, the adapter server must not allow interactive login.
- Use HTTPS if a separate network segment for the adapter server and security server cannot be assigned. In such case, the communication is encrypted. To use HTTPS, certificates must be created for the adapter server and loaded in the security server.

If HTTPS is used, authentication is performed on both client (security server) and server (adapter server) side. To make it possible for the security server to verify the partner's authenticity, the adapter server's certificate must be loaded in the security server. Both self-signed and commercial certificates can be used.

The selected protocol applies to all defined adapter servers; that is, it is not possible to specify HTTP or HTTPS for individual servers.

5.2 LOADING ADAPTER SERVER CERTIFICATES

Follow these steps.

1. On the **Configuration** menu, click **Servers**, then click **Adapter servers**
2. On the **Connection type** drop-down list, select **HTTPS***(this setting applies to all adapter servers)*
3. Select an adapter server and click **Load**
4. Click **Browse** and load the adapter server certificate from the disk. The file must be in the DER or PEM format and with *.der* or *.pem* extension, respectively.
5. Click **OK**, then click **Save**. The certificate fingerprint is displayed in the list.

To use mutual authentication, load the security server's certificate, which corresponds to the internal key, to the adapter server. If a previously generated certificate is available in the security server, its message abbreviation is displayed in the field "Security server certificate fingerprint"; if not, the text "Certificate lacking" is displayed.

To create a new internal key:

1. On the same page, click **Generate new key**.

2. Enter the security server's IP address and click **OK**. A new key is generated, the fingerprint of which is displayed in the field "Security server certificate fingerprint ";
3. Click **Export certificate** and save the file (*proxycert.tar.gz*, contains the certificate in PEM and DER format) to disk.
4. Transport the exported certificate to the adapter server and add it, or have it added, to the list of trusted certificates. Detailed instructions are available in the adapter server manual.

The security server uses the same internal key to communicate with the adapter server and the organization's information system. Therefore, if you change the existing internal network key, and the same security server is used over HTTPS both by the database and the organization, then you must reconfigure both the adapter server and the organization's information system.

5.3 SETTING ADAPTER SERVER PARAMETERS

Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Adapter server parameters**.
3. Fill in the fields as follows:
    - **IP**address – The adapter server's IP address
    - **Port** – The adapter server's port for receiving HTTP or HTTPS queries (for HTTP, the default is 80; for HTTPS, 443)
    - **URI** – The adapter server's directory and file name. For instance, if the adapter server's URL is *http://server/directory/file* then enter */directory/file* in the URI field.
    - **Schema URI** – The file containing the description of methods implemented in the adapter server. For instance, if the service descriptions' URL is *http://server/directory/database.wdsl* then enter */directory/database.wsdl* in the field. NB! To use XForms, see the note at "Schema URI" in section 4.3.
    - **Maximum time to process one incoming query (sec)** – Self-descriptive, but note: choose a time value that exceeds the total time spent for processing the query in the adapter server and exchanging the query between security servers. ***If the query or the response is a SOAP message with attachments, the time limits are switched to another mode***, wherein this value specifies the maximum pause allowed to occur in the data exchange. NB! Switching will take place only after sending the first sub-part of a query with attachments (SOAP message). This means that, in case of a regular query and response with attachments, the adapter server shall send at least the beginning of a message with attachments during the period specified herein. Similar general limit applies also to the organization's security server – it may be necessary to extend the limit of the organization for processing slow (large) queries.
    - **Heartbeat query interval (sec)** – The interval between test queries that check whether the database is operational. Enter *0* (zero) to switch off the check.
4. Click **Save**.

5.4 REMOVING ADAPTER SERVER

If you want the security server to not send any queries to the adapter server, change the adapter server parameters as follows.

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select the database to be removed, and then click **Adapter server parameters**.
3. In the **IP** field, enter *0.0.0.0***.**
4. Empty the field **Adapter server URI**.
5. Click **Remove ACL database**. The access rights of the database's organizations are emptied, after which none of the organizations can query the database. **Attention:** this action cannot be undone.
6. Click **Save** to apply the changes**.**

5.5 MANAGING ACCESS RIGHTS

For organizations to make queries to an X-Road database, they must have signed an agreement with the database in question. Access rights are controlled at the database's security server and granted to organizations as a whole; individual employees are authorized at the organization's information system.

Attention: Valid access rights control within the organization's information system is a prerequisite for joining X-Road.

Access rights can be managed in two modes:

- The **Show by groups** mode (default) allows to assign one or more queries to a single organization or group. Use this mode if you want to change something about a particular organization, for example, signing or annulling a data use contract with the organization.
- The **Show by queries** mode allows to specify one or more organizations/groups that can perform one particular query. Use this mode if you want to change the rights pertaining to a certain query, for example, if a new query is added to the adapter server or if related access rights should be revised due to the change of security requirements related to the query.

5.5.1 Setting access rights (Viewed by organizations)

To open the access rights management page:

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Access rights***(requires a configured adapter server; otherwise, the button is disabled)*.Two columns are displayed: one contains a list of groups/organizations (empty, if it has not been loaded from the adapter server), the other contains a list of queries supported by the adapter server.

(1) SETTING ACCESS RIGHTS

Assuming that the access rights management page is opened, follow these steps.

1. Click **Add** to select organizations for granting access rights. You can choose from the list containing all subjects registered in the X-Road central agency. By default, only groups are displayed; to also display organizations, select the **Show organizations** checkbox.
2. Click all applicable groups/organizations, and then click **OK**. The selected subjects will be displayed in the list (groups in blue, organizations in black).
3. Click **Refresh** to load a list of supported adapter server queries to the security server.
4. Grant access rights for organizations/groups: on the leftmost list, select organizations or groups, and on the rightmost list, select the checkboxes for queries that the subject is allowed to perform. If query encryption is also needed, see instructions in chapter 7.5.
5. Click **OK** to apply the changes.

For troubleshooting, refer to chapter **4.4.3 Troubleshooting**.

Attention: If you make changes to access rights, the **Refresh** button will be disabled until the changes have been either saved or canceled.

(2) CHANGES IN ACCESS RIGHTS ON REFRESH

If after refreshing the query list it appears that a query, which is assigned to an organization, has been removed from the adapter server, a warning is displayed and you will have to choose between two options:

- If you choose **Remove access rights**, all access rights pertaining to this query are removed;
- If you choose **Keep access rights**, the query will be removed from the list of supported queries, but the pertaining organization access rights are retained in case the query becomes supported again in the future.

(3) ENCRYPTED QUERIES

Attention: This section may only apply to servers registered in Estonia.

For every query, you can specify whether the selected organization can perform it with encryption (not applicable to groups). To enable or disable encryption for a particular query, click **Allow query encryption**. A lock icon is displayed next to encrypted queries.

Note: Allowing encryption in this dialog is only one of many prerequisites. In order for the encryption to actually work, the following conditions must be met:

- The organization has received a permission from the X-Road central agency to encrypt queries, and added to a special group in the certification authority;
- The query contains an encryption request;
- The X-Road central agency has provided the security server with an encryption key (more information can be obtained when applying for an encryption permit).

(4) EXPORTING ACCESS RIGHTS LISTS

To export the access rights list to a text file:

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Access rights**.
3. Select a group/organization and click **Export** to save the selected group's/organization's access rights
   –or–
   Click **Export all** to save all access rights.

The access rights are saved to the file *proxy_acl.txt* in the following form:

```
TestOrganization            orgtest
      populationregister.query1
      populationregister.query2
      populationregister.query5
CitizensPortal              portal
      populationregister.query2
      populationregister.query6
PoliceAgency              70000728
```

5.5.2 Granting access rights (View by queries)

The mode is similar to granting access rights by organizations, with the difference that for every query, one or more groups or organizations can be selected that have the right to perform the query in question.

The exported access rights list is also different, containing a list of queries and, under every query, a list of organizations allowed to perform the query.

5.6 ACCESS RIGHTS SYNCHRONIZATION IN A SECURITY SERVER CLUSTER

5.6.1 Introduction

The system provides three access rights list (ACL) synchronization methods.

- **Independent** (default) – access rights are not synchronized; database ACLs are changed only through the current security server's user interface; and the database's security server does not share the ACLs with other security servers.
- **Master** – enforces its access rights to all slave servers. The master server has a list of security server's (external) IP addresses where ACL synchronization messages will be sent. **Note that synchronization is always performed manually**.
- **Slave** – receives access rights from the master server; synchronizes itself upon receiving an ACL synchronization message.

For every database's security server, the last ACL configuration checksum is displayed. The valid ACL configuration checksum of a database is always displayed, irrespective of ACL administration type.

5.6.2 Slave server

If you select the "Slave" role, only the access rights checksum is displayed. All other operations with access rights are disabled (i.e., in a read-only mode).

ATTENTION

Upon restoration of a slave-type security server, access rights for every database shall be synced in its master.

5.6.3 Master server

If the "Master" option is selected, the following new options appear:

- **Add** – allows to add new slave servers by their IP addresses;
- **Remove** – removes the selected slave server;
- **Synchronize** – synchronizes the ACL with the selected slave;
- **Synchronize all** – synchronizes the ACL with all slaves.

For every slave, the ACL checksum of the last successful synchronization attempt is displayed (i.e., it may not conform to actual access rights of a slave, if e.g. older configuration has been restored in the slave). If synchronization fails, the slave's checksum is highlighted in red.

ATTENTION

Upon restoration of a master-type security server, access rights for every database shall be synced.

5.7 MANAGING AGGREGATE DATABASE FOR THE ENCODING SERVICE

5.7.1 Introduction

Starting from version 5.0, X-Road security servers are equipped with a pseudonymization ("encoding") service to allow the performance of anonymous aggregate analyses. The service encodes sensitive information present in query responses so that any personal information is impossible to extract or detect, while allowing an aggregate database to be built from the data received from multiple source databases. One database can belong to several aggregate databases simultaneously.

As the pseudonymization service is provided by the database's security server, there is no central vulnerable point in the system that would possess all the pseudonymization keys or see all delicate information in the clear. An aggregate database, in the X-Road context, is the same as an organization; it makes queries to source databases and aggregates the pseudonymized data received.

Within one aggregate database, one **pseudonymization key** is used. The linking of pseudonymized data is what allows an anonymous aggregate database to be created. The

database key is manually distributed to all source databases of that aggregate database, by way of generating the key in any of the databases and loading the key to all other databases. The pseudonymization key is transported to security servers on physical media.

5.7.2 Managing encryption keys

When exportinga pseudonymization key, you can choose the database for which the key is exported. Before downloading, the key is encrypted with the selected database's security server public key and additionally signed with the local security server's valid private key.

When importing a pseudonymization key, you can choose the database from where the key is imported. On importing, the key signature is verified against the certificate of the security server that exported the key, and decrypted using the security server's current or new private key. The decrypted key is saved in the security server's configuration and put to use immediately.

There is no key exchange functionality, since an aggregate database basically equals a pseudonymization key, i.e., by generating a new key, a new aggregate database is created.

5.7.3 Creating new aggregate database

Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**, select a database, and then click **Aggregate databases**.
2. Click **Add**.
3. Enter a short name and description for the aggregate database.
4. Choose to generate a new pseudonymization key.
5. Click **Save**.

5.7.4 Adding new aggregate database

Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**, select a database, and then click **Aggregate databases**.
2. Click **Add**
3. Enter a short name and description for the database
4. Choose to import the pseudonymization key.
5. Select the database where the key will be imported from
   –or–
   Load the key from the disk.
6. Click **Save**.

5.8 REMOVING THE DATABASE'S SECURITY SERVER FROM X-ROAD

If you want to stop providing data over X-Road, and if the security server serves only one database, then do the following.

1. Inform the central server's administrator that the security server's certificates need to be revoked;
2. Remove the security server from the network;
3. Destroy the security server private keys by wiping the server's hard disk.

However, if you need to keep the security server running, because it serves other databases or units in the organization, you only need to revoke the database's certificates. Follow these steps.

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Keys**.
3. Write down all certificate fingerprints and transmit them to the central server's administration with a request to revoke the certificates.
4. Click **Cancel** to return to the list, then click **Remove database**. After confirmation, the private key for servicing the database, the certificates, and the respective adapter server configuration together with its access rights will be removed from the security server.

6 MANAGING ORGANIZATION'S SECURITY SERVER

6.1 OVERVIEW

An organization that has joined X-Road installs a security server to perform queries from its information system to X-Road databases. For this to work, specify the settings for communication between the information system and a security server. This section describes the necessary activities for configuring the information system (subsection 6.2) and the security server (all other subsections).

6.2 CONFIGURING INFORMATION SYSTEM SERVER

In order for the information system to use the security server to perform queries, the information system must be initialized with the main parameters of the security server.

- **IP address** – the security server's internal IP address.
- **Port** – Enter *80* for HTTP, *443* for HTTPS.
- **URI** – Enter */cgi-bin/consumer_proxy.*
- **HTTPS certificate** – see 4.3.

Setup of information system is described in "Requirements for Information Systems and Adapter Servers" [http://x-road.ee/docs/eng/x-road_service_protocol.pdf]

6.3 ORGANIZATION'S INFORMATION SYSTEM PARAMETERS

6.3.1 Introduction

The security server can communicate with an information system (IS) server over HTTP (the default) or HTTPS.

- Use HTTP if both the IS server and the security server communicate in a network segment where no other computers are connected to. Also, the IS server must not allow interactive login.
- Use HTTPS if a separate network segment for the IS server and security server cannot be assigned. In such case, the communication is encrypted. To use HTTPS, certificates must be created for the IS server and loaded in the security server **Attention:** In this case, authentication is performed on both the client (IS server) and the server (security server) side.

6.3.2 Configuring for HTTPS

Load the IS server certificate:

1. On the **Configuration** menu, click **Servers**, then click **Information system servers**.
2. Select an organization, from the **Connection type** drop-down list select **HTTPS**, and then click **Load**.

3. Click **Browse** and load the IS server certificate from the disk. The file must be in the DER or PEM format and with the *.der* or *.pem* extension, respectively.
4. Click **Save**. On success, the certificate's fingerprint is displayed in the list of the organization's certificates.

In the security server, a key must be generated for communicating with IS servers, and the corresponding certificate loaded to IS servers.

Generate the key used for local network communication:

1. On the same page, click **Generate new key**.
2. Enter the security server's domain name and internal IP address; click **OK**. The security server generates a key for the communication with information system servers and adapter servers, as well as a respective self-signed certificate. As a result, the security server's certificate fingerprint also changes. The entered domain name is saved in the field Common Name of the certificate and IP address in the extension field subjectAltName of the certificate;
3. Click **Export certificate** and save the certificate to disk.
4. Click **Save**.
5. Transport the exported certificate to the IS server and add it, or have it added, to the list of trusted certificates.

The security server uses the same internal key to communicate with the adapter server and the organization's information system. Therefore, if you change the existing internal network key, and the same security server is used over HTTPS both by the database and the organization, then you must reconfigure both the adapter server and the organization's information system.

6.4 REMOVING ORGANIZATION FROM X-ROAD

If you wish to remove your organization from X-Road, and the security server is used by one organization only, follow these steps.

- Ask the central server's administrator to revoke the security server's certificates;
- Remove the security server from the network;
- Destroy the security server's private key by wiping the hard disk.

However, if you need to keep the security server running because more organizations use it, do the following.

First, to remove an organization from X-Road, its certificates must be revoked. To do that, send to the central server's administrator a list of certificate fingerprints and remove the corresponding private key from the security server's disk.

Follow these steps.

1. On the **Configuration** menu, click **Organizations**.
2. Select an organization, and then click **Manage organization keys**.

3. Write down all certificate fingerprints and send them to the central server's administrator, requesting for revocation.
4. To remove the organization's private key, click **Remove organization** and click **Yes** in the confirmation dialog. The organization's private key and certificates will be removed.

7 KEY EXCHANGE WITH EXTERNAL SUBJECTS

7.1 INTRODUCTION

During the operation of the security server, it may become necessary to change one of the following keys:

- The DNS key;
- The certification authority key;
- The key used by the security server to sign queries and secure communications.

Key change can be either:

- Regular change – the key is changed periodically (for example, annually) to minimize the risk of exposure;
- Emergency change – the key and all its back-ups have been destroyed or the key has been exposed.

To ensure smooth key change while maintaining the continuous operation of X-Road, all keys that involve external subjects are changed in several stages. Typically, the adoption of new key includes the following steps:

- The party requesting change generates a new key for themselves and sends it to their communication partners;
- Communication partners enter the new key in their system and start accepting queries and communication sessions related to the new as well as old key in parallel;
- When it is confirmed that all communication partners have received the new key, the party requesting key change will actually introduce the new key;
- After the new key is introduced, the communication partners delete the old key from their system.

This procedure ensures continuous operation of the system also during key change.

7.2 CHANGING THE DNS KEY

7.2.1 Overview

To ensure the authenticity of security server information distributed over DNS, the central server signs all DNS records. To verify the records, a security server must have the central server's public key, which is loaded in the security server over HTTP. To verify the downloaded key, the security server's administrator will receive the key's fingerprint from the central server's administrator, and enters it in the security server.

To allow for a smooth DNS key change, it is carried out in several phases.

1. The central server's administrator generates a new DNS key and transmits its fingerprint to all security server administrators. (DNS keys are still signed with the old key.)
2. The security server administrators enter the new key fingerprint. It enables the servers to trust DNS records signed with either of the keys.

3. After verifying that all security servers use the new key, the central server's administrator switches over to the new key (effectively making it current). The old key is removed in the process.
4. All security server administrators remove the old key from their servers. With that, the security servers will trust DNS records signed with the new (current) key only.

The following two sections contain instructions on performing the steps 2 and 4 (steps 1 and 3 are performed by the central server's administrator).

7.2.2 Adding new DNS key

To load a new key to the security server, you must know the fingerprint of the new key.

1. On the **Configuration** menu, click **Keys and certificates**, then click **DNS keys**.
2. Click **Add new key**.
3. Enter the central server's IP address and the key fingerprint received from the central server's administrator (in the form XX:XX:XX...), then click **OK**. On success, the fingerprint will be displayed on the list.

NB! When entering fingerprint, enter also the colons included in the code; uppercase and lowercase letters are not differentiated when entering letters.

If downloading the key failed, relevant error message is displayed. A "404 Not Found" error indicates that the fingerprint was invalid.

7.2.3 Using new DNS key

Follow these steps.

1. On the **Configuration** menu, click **Keys and certificates**, then click **DNS keys**.
2. Click **Remove old key**.
3. Click **Save**.

7.3 CHANGING CA KEYS

Security servers use public key cryptography during communication with their partners to ensure secure communication. For easier distribution of keys, the certificates are issued by the certification authority (CA) at the X-Road central server. To verify the certificates, a security server must possess the CA's self-signed certificate, which is loaded from the central server over DNS (assumes a correctly configured name service). To avoid loading the wrong keys, the central server's administrator provides the security server's administrator with the CA key fingerprint that must be entered in the security server.

To allow for a smooth CA key change, it is carried out in several phases.

1. The central server's administrator generates a new CA key and the corresponding self-signed certificate. All security servers are issued certificates signed with the new certification key. The central server's administrator announces the new certificate's fingerprint to all security server administrators.

2. The security server administrators enter the new key fingerprint, which enables their servers to communicate with other security servers that use either the old or the new certificate.
3. All security servers put the new certificate to use while continuing to accept certificates signed with the old key.
4. The central server's administrator revokes the old key and certificates issued with it.
5. Security server administrators remove the old certification key and begin to accept only certificates issued with the new key.

The following subsections contain instructions on performing steps 2, 3, and 5 (steps 1 and 4 are performed by the central server's administrator).

7.3.1 Adding new certification key

Follow these steps.

1. On the **Configuration** menu, click **Keys and certificates**, then click **CA certificates**.
2. Click **Add new**.
3. Enter the certificate fingerprint received from the central server's administrator and click **OK**. The server will be downloaded and added to the list in the state "New". After performing this step, the security server can exchange messages with other security servers using either the old or the new CA certificate.

If an error occurs:

- The error message "Empty answer from DNS server" indicates that the CA certificate has not yet been loaded to the central server. Notify the central server's administrator.
- The error message "Cannot load new certificate for the security server key" indicates that re-issuing all security server certificates with the new certification key has failed. Notify the central server's administrator.

7.3.2 Using new certification key

After all security server administrators have entered the new certification key, new certificates issued with the new certification key must be activated. This doesn't have to occur in all security servers simultaneously, as old and new certificates can be used in parallel.

1. On the **Configuration** menu click **Keys and certificates**, and then click **CA certificates**. Two certificates are displayed, one of which has the status "Current" (i.e., currently in use) and another which has the status "New" (i.e., supported, but not in use yet).
2. Click **Use new**. The status of the current certificate is changed to "Old" and that of the new certificate to "Current", thus ensuring that message exchange with other security servers can continue even if they haven't activated the new certificate.

7.3.3 Removing old certification key

The old certification key can be removed only after all security servers have activated the new certification key.

1. On the **Configuration** menu, click **Keys and certificates**, then click **CA certificates**.

2. Click **Remove old key**.

7.4 CHANGING THE SECURITY SERVER KEY

In the following cases, security server's key must be changed:

- when the key becomes compromised;
- when the key is destroyed (and there is no back-up copy of the configuration);
- when regular, annual key change is performed to reduce the risk of key compromise.

In the first two cases, an emergency key change is performed, which consists of the following steps.

1. The security server's administrator transmits to the central server's administrator the list fingerprints of certificates issued with the compromised or destroyed key;
2. The central server's administrator revokes the certificates in question;
3. The security server's administrator generates a new key and certificate request;
4. The security server's administrator transmits the certificate request to the central server's administrator;
5. The central server's administrator issues a new certificate based on the request;
6. The security server's administrator loads and activates the new certificate.

Regular key change consists of the following steps.

1. The security server's administrator generates a new key and certificate request;
2. The security server's administrator transmits the certificate request to the central server's administrator;
3. The central server's administrator issues a new certificate based on the request;
4. The security server's administrator loads and activates the new certificate.
5. The security server's administrator transmits to the central server's administrator the list of fingerprints of certificates issued with the old key;
6. The central server's administrator revokes the certificates issued with the old key.

7.4.1 Creating new key

In the organization's security server:

1. On the **Configuration** menu, click **Organizations**.
2. Select an organization and click **Keys**.
3. Click **Generate new key**. “Available” is displayed on the line "New key".
4. Save the certificate request file *(certreq.gz)* to disk.
5. Click **Save**.

In the database's security server:

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select database and click **Keys**.
3. Click **Generate new key**. “Available” is displayed on the line "New key".
4. Save the certificate request file *(certreq.gz)* to disk.

5. Click **Save**.

In both cases, transmit the certificate request to the central server's administrator together with the organization's official name and registry code.

7.4.2 Loading and using security server certificate

After the central server's administrator has issued a new certificate for the organization and entered it in the DNS database, the security server can put the certificate to use.

Attention: As all security servers cache the X-Road DNS database, allow at least four hours until the certificate has reached all parties. Therefore, it is recommended to wait at least 4-6 hours after the certificate has been issued before activating it.

7.4.3 Activities if the key is compromised or destroyed

If the security server key becomes compromised or destroyed, transmit to the central server's administrator a list of fingerprints of the certificates issued with this key for revocation. Follow these steps.

In the organization's security server:

1. On the **Configuration** menu, click **Organizations**.
2. Select an organization and click **Keys**
3. From the **Valid key** group, copy the fingerprint on the **Certificate** field and transmit it to the central server's administrator.

In the database's security server:

1. On the **Configuration** menu, click **Databases/Registries**.
2. Select a database and click **Keys**.
3. From the **Valid key** group, copy the fingerprint on the **Certificate** fieldand transmit it to the central server's administrator.

7.5 QUERY LOG ENCRYPTION AND SECURITY SERVER ENCRYPTION KEY CHANGE

7.5.1 Encryption in security server

In X-Road, query logs can be encrypted in three different ways, one of which (encryption with the ID card authentication certificate) is outside the scope of this document. The other two methods are explained below.

(1) ENCRYPTION WITH THE CENTRAL SERVER KEY

Encryption with the X-Road central server's key is only performed in the database's security server; and the procedure goes as follows.

1. The organization requests from the X-Road central agency a permission to perform queries encrypted with the central server's key.
2. Upon receiving the permission, the organization applies for an agreement with the database owner to encrypt queries to certain services.
3. The owner of the database decides whether to sign the agreement; if necessary, requesting legal reasons from the organization.
4. If an agreement is reached, then the queries that the organization performs to a certain service are logged in encrypted form in the database's security server.

Hence, plaintext information about the query exists in the database information system only in the moment when the query is performed; later, it is impossible to determine whether such a query was ever performed. The key for decrypting queries is in the possession of an authorized supervisory body, who can decrypt the logged query if necessary. If query encryption fails (e.g. encryption is not permitted), an error message is returned.

Note: This encryption mode assumes that the central server's public key is loaded in the database's security server.

(2) ENCRYPTION WITH THE SECURITY SERVER KEY (LOCAL ENCRYPTION)

Logging messages in plaintext involves several risks. For example, the security server administrator and other persons with an access to the server can in theory see the contents of messages; and if archived copies are stolen or copied, attackers can see all archived queries and responses.

To minimize risks, all X-Road security servers log all queries in encrypted form; furthermore, all logs are encrypted (so-called first level encryption). Queries are encrypted with the security server's special encryption key, both in the database and information system security server. To use query encryption, an encryption key must be generated in the security server and the encryption option turned on (see below).

If the security server is set to encrypt queries (this is a local setting not reflected in the queries), then the key is used for encrypting all those queries *not intended for encryption with an ID card*. If the security server is unable to secure the query, it is neither processed nor logged, and the performer of the query is returned an error message. If the server uses local encryption and receives a query requesting encryption, then the query is encrypted the second time using the X-Road central server key (assuming all the prerequisites are fulfilled).

7.5.2 Creating and changing encryption key

For the security server to encrypt logged queries, a special encryption key must be generated in the security server. The key is generated by the security server administrator in the presence of a security officer, and exported to removable media (floppy disk, CD, DVD or USB memory stick).

To generate an encryption key:

1. On the **Configuration** menu, click **Keys and certificates**, then click **Encryption key**.

2. Select the **Use local encryption** checkbox, which turns in the encryption functionality. If local encryption is not used, queries are logged as plaintext.
3. Click **Generate new key**. The system will generate a new key pair and updates the CN (Common Name) and SN (Serial Number) fields. When the validity of a query is proved, the key is searched by these two parameters.
4. Save the key file to disk (*localseal.tar.gz*, containing the key pair's private key part).
5. Click **Save** to use (activate) the new key.
6. Make at least two copies of the saved key file to different media.

Attention: The exported key is used for decrypting encrypted log files in case a query's legality needs investigation. Therefore, removable media containing copies of the key must be stored in a safe and secure place according to organizational rules.

8 ADDITIONAL SYSTEM CONFIGURATION

8.1 CHANGING SECURITY SERVER'S IP-ADDRESS

Upon initial installation of the security server, IP addresses of external and internal interfaces are added automatically into its configuration. If either address is later changed in the system (from command line or Ubuntu graphic interface), this will not make automatic correction in the security server. To ensure that changes reach the security server, a command shall be given on the command line:

```
sudo dpkg-reconfigure xtee-proxy
```

8.2 BACKING UP CONFIGURATION

Regular back-up copies must be made of the security server's configuration. Follow these steps.

1. On the **System** menu, click **Back up configuration**.
2. Click **Back up configuration** and wait until files are prepared for archival. The name of the archive file is in the form *conf_backup_YYYYMMDD-hhmmss*, where YYYY denotes the current year, MM – month, DD – date, hh – hour, mm – minute, ss – second.
3. For security purposes, save the archive file directly to removable media and store it in a secure place, such as a safe. Do not save the file on the local computer.

Notes:

As of version 5.31, configuration is backed up automatically in every 15 minutes, if any changes have been made in the configuration, in the directory /usr/xtee/var/backup. Configuration archives with 7 different changes are stored. File name of the backed-up configuration is in the confbackup_type_hostname_IP_YYYYMMDDhhmmss.tar form, where type is X-Road server type (proxy, ca, monitor, central), hostname and IP is hostname of relevant server and IP address, through which routing to Internet takes place, YYYY – back-up year, MM - month, DD - date, hh - hours, mm - minutes, ss – seconds.

The back-up copies of the security server's configuration include, among other things, the private keys for signing queries and securing data exhange. Therefore, make sure that the confidentiality of the back-up copies is preserved.

8.3 RESTORING CONFIGURATION FROM BACK-UP COPY

Proceed as follows:

a. In the **System** menu select **Restore configuration**;
b. Click **Browse** and select configuration file used for restoration;
c. Click **Restore configuration.**

After the configuration has been restored, immediately change central server's IP address and DNS key (as these are different in every X-Road 5.0 environment), then select the command

Reconfigure all in the Configuration menu. In order to check correctness of the restored configuration, in the menu System select Diagnostics and then Test all. When all tests are successful, configuration of the security server has been restored successfully.

ATTENTION

If restoring from back-up copy is used for cloning the security server, a new key must be also generated for the monitoring system! Proceed as described in section 9.6 CHANGING MONITORING SYSTEM KEY.

ATTENTION

In case of a security server in a cluster, access rights must be synced as well. In case of a slave security server, access rights must be synced in the master security server. In case of a master security server, its slaves must be synced. Synchronization is database-based, i.e. if the security server includes several databases, these must be accessed one by one after restoration, and synchronization of access rights must be activated in every database.

8.4 CONFIGURING TIMEOUTS AND LOGGING

To open the page, click **Configuration**, then click **Timeouts and logging**, and set the following parameters.

- **Maximum duration of queries (in seconds) to the database.** Specifies how long the security server will wait for a query result from a database. If the query or response is a SOAP message with attachment, this value is used as the maximum allowed pause between transmissions of data. Note: For a normal query with a response with attachments, the switching takes place after the database's security server has transferred the first part of a multi-part message. Therefore, during the period specified here, all databases that send responses with attachments should at least begin sending the response.
- **The interval of sending log hashes to central server (in seconds).** The period after which log file hashes are sent to the central server. Recording entries in the central server ensures later proof value of queries. The minimum period is 360 seconds (six minutes), as more frequent sending would be considered a denial-of-service attempt by the central server, and as such ignored.
- **The interval of log file sync. to disk (in number of log records).** After every Nth record, the log file buffers are written to disk to minimize data loss in case of a system crash, and to ensure easy continuation of the hash chain. Set the interval to 1 to turn off buffering (i.e., write files to disk synchronously).
- URL for automatic archiving of query logs, HTTP method and allowing log zipping. Archiving with HTTP protocol is described in detail in section 8.8 "Archiving query logs".
- **Interval between first and second send attempts (in seconds)**. If sending fails, the second attempt is made after the time specified here has elapsed. Every next attempt doubles the pause.
- **Maximum interval between send attempts (in seconds).** If the second attempt also fails, then the pause between every following attempt is increased, but no more than the value specified here. The value of this parameter is the length of maximum interval in

seconds. If length of the pause would become longer than maximum allowed pause, this maximum value is used.

- **Maximum number of messages processed in parallel.** Specifies the number of messages sent in one attempt. Only messages to different databases can be sent simultaneously.
- Fingerprints of certificates of log archiving servers. Alternative for log archiving on disk is their forwarding to a server dealing with archiving, using HTTPS protocol. In order to ensure authenticity of the server receiving logs, fingerprint of this server must be loaded to the security server. If a certificate is successfully imported, the certificate fingerprint is displayed in this field. See also section 8.8 ARCHIVING QUERY LOGS.

8.5 EXAMINING SYSTEM LOGS

Follow these steps.

1. On the **System** menu, click **System log files**.
2. Click the name of the log file in the upper row to display its contents (max. 1000 newest lines).

To send a log file by e-mail (e.g. for troubleshooting), enter an e-mail address in the box below the log window and click **Send**. The feature assumes that the security server is configured to send e-mail.

8.6 MAIL FORWARDING

For easier monitoring of the system, the mail for *root* and *postmaster* accounts can be forwarded to another e-mail address.
Follow these steps.

1. On the **System** menu, click **Mail forwarding**.
2. Enter the e-mail address where system mails are forwarded
   –or–
   Empty the field to stop mail forwarding
3. Click **Save**.

The change will take effect after reconfiguration of the security server (select the command Reconfigure all in the Configuration menu).

8.7 UPDATING SECURITY SERVER

Starting from version 5.0, the X-Road servers (including security server) no longer use a custom patching mechanism. Instead, new versions are distributed through the X-Road package repository, where updates can be loaded through the command line (apt-get) or with a graphical package manager (Ubuntu Synaptic).

In order to load new version from command line (assumed that repository address is set according to section 2.4), enter:

```
sudo apt-get install xtee-proxy
```

In order to return to older version, enter on the command line:

sudo apt-get install xtee-proxy=5.0,

where "5.0" must be replaced with the required version number.

8.8 ARCHIVING QUERY LOGS

8.8.1 Introduction

The security server stores all received messages (queries or responses) to a query log. As the log files grow over time, they need to be archived periodically and removed from the server. For this purpose, the security server allows sending log files to a log server. The following options are available.

- Sending log files to a log archival server over the network (HTTP or HTTPS) manually.
- Sending log files to a log archival server over the network (HTTP or HTTPS automatically. Archiving takes place automatically, if sufficient amount of data has accumulated.

Consider that log records may contain confidential information, and therefore apply the same security precautions that would be applied in the adapter server or organization's information system for handling sensitive data.

If network archival is used, both PUT and POST methods are available. The PUT method is used according to the HTTP/1.1 standard (RFC 2616). With the POST method, the log server will be sent the following HTML element:

```
<input name=”fail” type=”file”>
```

The message body sent to the log server is of type *multipart/form-data*. The name of the file to be sent is described in the relevant *Content-Disposition* header with the attribute *filename*. For more information, see RFC 1867.

If the archival URL contains the string "%f" then it will be replaced with the actual filename to be archived, comprising the date and time of archival with millisecond precision.

If HTTPS protocol is used, log server certificate must be loaded into the security server and log URL must start with the string "https://". Certificate can be loaded from the menu Configuration -> Timeouts and logging (see 8.4 CONFIGURING TIMEOUTS AND LOGGING). In addition, the key of the security server itself and relevant certificate must be generated. Key can be generated from the menu Configuration -> Information system servers or Configuration -> Adapter servers, clicking "Generate new key". When a key has been generated, press "Export certificate", save it to the disk and configure the log server, where queries will be archived, to ensure that it will accept the certificate. Web server must be installed in log server with the following cgi script: http://x-road.ee/scripts/sslog-archive.cgi.gz. If HTTPS protocol is going to be used, it must be configured as a standard in log server.

8.8.2 Archival to disk

Follow these steps.

1. On the **System** menu, click **Archive query logs**.
2. Select **Archive to disk** and click **Archive**. The logs are rotated and prepared for downloading.
3. Save the file to disk.
4. Select whether to remove the archived log files from the security server or keep them. Keeping logs enables making current back-up copies of more recent log files and to delete the files only when a whole CD or DVD with data can be archived.

8.8.3 Manual archival over network

Follow these steps.

1. On the **System** menu, click **Archive query logs**.
2. Select **Archive to another server over HTTP**
3. Enter the archival server URL, select access method (PUT or POST), and select whether to compress the log files with GZip before archiving.
4. Click **Archive**. The logs are rotated and prepared for sending, and then all files are sent to the archival server. The operation is atomic, i.e., if transmitting one file fails, the whole operation fails and next time, the system will again try to send all files.

8.8.4 Automatic archival over network

Follow these steps.

1. On the **Configuration** menu, click **Timeouts and logging**.
2. In the **Automatic archival of query logs** group, specify the following:
    - The automatic archival URL for log files;
    - HTTP access method (PUT or POST);
    - Whether to activate automatic archival;
    - Whether to compress the log files with GZip before archival;
    - The archival server certificate (needed only if logs are archived over HTTPS; see also 8.4 CONFIGURING TIMEOUTS AND LOGGING)

The query logs are automatically archived:

- when the log daemon (sslogd) is restarted,
- when the log daemon is sent the HUP signal,
- or when the log file grows larger than about 20 MB.

If archival over network is used, the query logs of different security servers can be sent to the same directory, as the archive file is prefixed with the security server's hostname (e.g.*myproxy-20100903-144835-1283514515-713867.gz*).

9 MONITORING

9.1 OVERVIEW

X-Road is equipped with a monitoring system that allows system administrators to get timely information about the status and operability of security servers under their control, and to quickly react to various problems, such as communication disruptions, hardware malfunctions, software problems, etc.

Security server is usually located in a server room, where the system administrator is not staying constantly and therefore cannot get enough information about the status of the server. Therefore, X-Road is equipped with a monitoring system providing to the system administrators operative information about the status quo and usability of the security servers in their administrative area.

To collect information from security servers, a single special-purpose server, called the local monitoring station, is connected to X-Road. Local monitoring station receives monitoring information from the security servers in the administrative area of the system administrator. In addition, it is possible to use standard SNMP monitoring software (such as Nagios) that receives and displays SNMP *trap* messages from the security server.

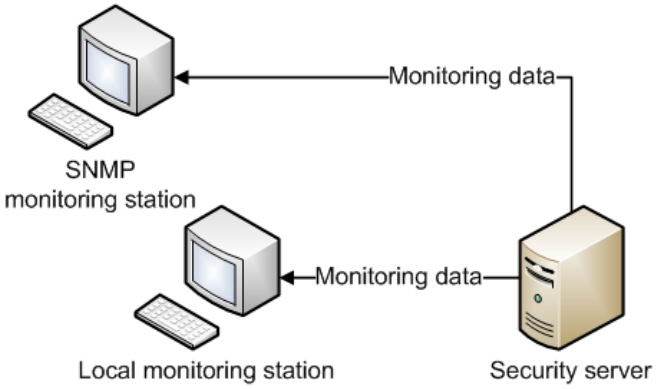


Figure 2. Collecting information from servers

Security servers and central servers send three types of messages to monitoring stations:

- Status information – CPU load, free memory, etc;
- Error messages – if an error occurred during query exchange, relevant message is sent to the monitoring station.
- Query information – for every query exchanged, the complete information from its header (originating agency, official's personal ID code, database name, query name) is sent to the monitoring station, allowing to gather statistics about query popularity and detect possible misuses

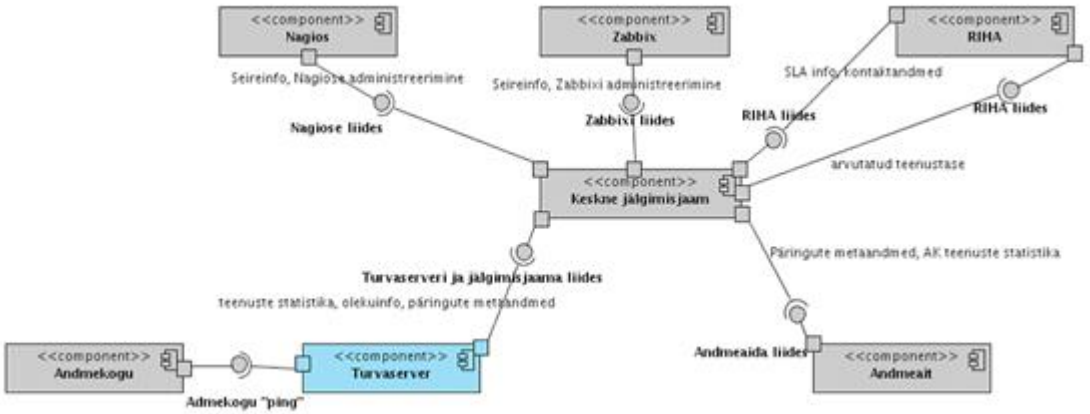
The information exchanged between the security server servers and the local monitoring station is encrypted using a special key. The key is distributed over DNS. The security server sends its monitoring key automatically to the central server where it is linked to all organizations in the

security server, and added to DNS. The key of the local monitoring station is transported on removable media to the security server, and loaded there.

The communication between the security server and the SNMP monitoring station is public. As the information is not encrypted, no sensitive messages (i.e., query statistics) are transmitted over the SNMP protocol either.

9.2 EXTERNAL MONITORING SYSTEMS

In addition to local and central monitoring stations, as of version 5.2 (09.2012 pack), the security server communicates also indirectly with external monitoring systems Zabbix and Nagios. Figure 3 shows location of the security server in more general X-Road monitoring infrastructure (see the document “Specification of new monitoring system of X-Road 5.0” [b]).



Monitoring information, Nagios administration

SLA information, contact data

RIHA interface

Calculated service level

Central monitoring station

Security server and monitoring station interface

Service statistics, status information, metadata of queries

AK service statistics

Database

Database “ping“

Data store interface

Figure 3. Security server in X-Road infrastructure

This does not mean any changes for an end user.

9.3 MONITORED PARAMETERS

A security server sends to all monitoring stations information about server status. Of this, the query statistics (i.e., who has performed what queries and how many times) is classified as sensitive information.

The following information is periodically sent to monitoring stations:

- **Version number** – security server's software version
- **Load** – average number of processes waiting for CPU time
- **CPU free** – free CPU time percentage (the same value that is displayed by *top*)
- **Connections waiting** – number of connections waiting to be serviced (size of the queue against denial-of-service), applies only to the database's security server.
- **Disk free** – free disk space in MB
- **Memory total** – total RAM in MB
- **Memory free** – free RAM in MB
- **Swap total** – total swap space in MB
- **Swap free** – free swap space in MB
- **Queries** – number of queries processed in the security server since the sending of the last message
- **Errors** – number of errors occurred since the sending of the last message
- **HTTP queries** – number of HTTP queries made to the central server since the sending of the last message
- **Log queries** – number of log records sent to the central server's log server since the sending of the last message
- **Traffic inbound** – bytes received during the period
- **Traffic outbound** – bytes sent during the period

For every query brokered, the security server sends to monitoring stations (except SNMP monitoring station) the following information:

- Name of the organization performing the query;
- Personal Identification Code of the person performing the query;
- Name of the query;
- Name of the database.

For every error, the security server sends to the monitoring station the following information:

- Error code – allows computerized processing of errors;
- Error text – a human-readable explanation.

9.4 MANAGING SNMP MONITORING STATIONS

An SNMP monitoring station runs standard SNMP monitoring software (e.g. Nagios) that receives and displays SNMP *trap* messages (see 12.1). This allows the system administrator more easily to

monitor several physically isolated servers. As the communication between the server and the monitoring station is public, no sensitive messages (i.e., query statistics) are exchanged.

To add a new SNMP monitoring station:

1. On the **Configuration** menu, click **Monitoring stations**, then click **SNMP monitoring stations**.
2. Click **Add**.
3. Enter the monitoring station's IP address and click **OK**. The new station will appear on the list.
4. Click **Save**.

9.5 MANAGING LOCAL MONITORING STATIONS

A local monitoring station is a special software built for X-Road to allow the system administrator to monitor the status and load of the security server independent of the server's physical location.

The communication between a security server and monitoring station is encrypted by means of the SKIP/ESP protocol. Therefore, both communicating parties need the other party's public key. The security server's monitoring system key is automatically generated on the server's installation and registered in the central server. In order to add a local monitoring station to the security server, load the stations key (generated in the monitoring station) from data medium (see also section 9.6 CHANGING MONITORING SYSTEM KEY).

To add a local monitoring station:

1. On the **Configuration** menu, click **Monitoring stations**, then click **Local monitoring stations**.
2. Click **Add**.
3. Enter the monitoring station's IP address (this must be available to the security server);
4. Click **Browse** and load the monitoring station's key (*key.gz*).
5. Click **OK**. The new monitoring station will be added to the list.
6. Click **Save**.

9.6 CHANGING MONITORING SYSTEM KEY

The communication between a security server and monitoring stations is encrypted with a dedicated monitoring system key, which is generated upon the security server installation. This key can be changed under normal or emergency circumstances. In the first case, the key is changed periodically, but infrequently, to reduce the risk of compromise. In the second case, the key is changed after becoming destroyed or compromised.

To generate and use a new key:

1. On the **Configuration** menu, click **Keys and certificates**, then click **Monitoring system key**.
2. Click **Generate new key**. The new key's fingerprint is displayed, but the key itself is not in use yet.

3. Click **Save** to use (activate) the key.

The new key is put to use immediately after saving, and also registered in the central server. The key appears in the DNS database in approximately ten minutes, after which the monitoring stations can decrypt data encrypted with the new key.

10 ASYNCHRONOUS MESSAGES

10.1 INTRODUCTION

Asynchronous messages are X-Road messages that do not need immediate response. When an asynchronous message is transmitted, it is stored in the organization's security server until the message is successfully sent or until the system administrator removes it from the queue. The organization's information system will immediately receive a receipt about the message's arrival, after which the sending of the message remains the responsibility of the security server.

Sending asynchronous messages is similar to sending e-mail, whereby the client program transmits the message to the mail server, which transmits the message to its destination as soon as possible. Sending an asynchronous message from the organization's information system to its security server succeeds even if the organization or database is at the moment of sending disconnected from the network.

A send attempt is considered successful if no communication errors occur and the response is not a Fault-type message from the adapter server. If the send attempt fails, the organization's system administrator is automatically notified of the problem over e-mail.

Asynchronous messages meant for a particular database are transmitted in the same order they arrived in the organization's security server. It also means that if a message could not be sent because the database's adapter server responded with an error, then the security server will continue trying to send the message, ignoring any other messages in the queue. In this case, the security server's administrator must investigate the problem and remove either the invalid message or all messages from the queue.

For every database, the security server has a separate message queue. This ensures that problems with one database won't affect messages to other databases.

Asynchronous messages are processed in the security server by a separate daemon. The daemon checks the queues of all databases with an approximately 10-second interval. If the first message of the queue is marked for removal (see below), it will be removed permanently. If sufficient time has passed between send attempts, the daemon will try to send the message again.

All send attempts and permanent removals are logged in the asynchronous messages' log (see section 10). The log files are rotated weekly, and at least the logs for the last four weeks are stored. Such logs are not included in the back-up.

The interval for send attempts is specified under **Configuration**>**Timeouts and logging** (see section 8.3). The message queue is managed through the asynchronous messages' manager (see section 10.2).

10.2 MANAGING ASYNCHRONOUS MESSAGES

To display asynchronous messages:

- On the **System** menu, click **Asynchronous messages**.

A window is displayed, providing overview of the status quo of message queues, showing output of failed attempts and enabling to remove messages from the queue.

The following information is displayed.

- **Database** – Full name of the database
- **Messages** – Number of unsent (queued) messages
- **Last attempt** – The message's last send attempt
- **Attempts** – Number of attempts to send the message
- **Next** – Time of next send attempt
- **Arrived on** – Time of arrival for the first message in the queue (this field and the previous one are applicable only if there are messages in the queue)
- **Short name** – Short name of the database.

If sending a message to the database fails, the following buttons become active:

- **Attempt output** – opens a window containing the output of the last attempt, which should provide information about the failure;
- **Zero send counter** – zeroes the send counter and the last send attempt time. Clicking this button immediately causes a new send attempt. NB! An attempt counter included in a log is also zeroed!

To change the status of a queued message:

- Click **Remove** to mark the message for removal
- Click **Restore** to restore the message in the queue.

The first message marked for removal is removed permanently from the queue as soon as the system re-checks the queue (usually within 10 seconds). A message cannot be restored after final removal.

10.3 LOG OF ASYNCHRONOUS MESSAGES

In the log of asynchronous messages, a new record is created for every send attempt or the final removal of a message.

11 ADVANCED

11.1 MANAGING WEB USERS

Upon installing the security server, the Web account "webadmin" is automatically created. To add other accounts, log in as "ui" and enter on command line:

```
/usr/xtee/www/script/newuser<account name><full name><password>
```

The account name must be a single word, while the full name can contain more, in which case it must be enclosed in double quotes, for example:

```
/usr/xtee/www/script/newuserjrd "John Richard Doe" 1234abcd
```

To change a user's password, enter the same command with a new password (You will be asked for confirmation):

```
/usr/xtee/www/script/newuserjrd "John Richard Doe" dcba4321
```

To remove an account, enter the following commands (You will be asked for confirmation):

```
sudo /usr/xtee/www/script/delwebuser<account name>
sudo /etc/init.d/apache2 reload
```

Attention: Web accounts are not shell accounts, i.e., they enable logging in only to the security server Web interface, not to the system.

11.2 IMPORTING DATA FROM VERSION 4

The new security server supports loading backups of older (4.0 series) security servers. Such a backup, however, must be compressed with TAR before it can be uploaded. In Windows, use the ported GNU Tar (http://gnuwin32.sourceforge.net/packages/gtar.htm); in Linux, the native "tar" utility. The name for the archive can be chosen freely.

Example (in Linux environment, it creates a correct archive file *backup.tar*, which is ready for loading through web interface). Precondition is that files are copied from data medium to a temporary directory /tmp/backup.

```
kasutaja@server:~$ cd /tmp


kasutaja@server:~$ ls backup/

backup.tar

backup.tar.sum

MD5SUMS
```

```
patchlevel

xteehosttype



kasutaja@server:/tmp$ tar cvf varukoopia.tar -C backup/ backup.tar \
backup.tar.sum MD5SUMS patchlevel xteehosttype
```

***Note**: Do not use the utility 7zip, which is known to produce broken TAR archives.

11.3 DIAGNOSTICS

X-Road is a dispersed system, the smooth operation of which requires cooperation of all components. Upon failures, it is usually difficult to find out, where the failure has occurred and how to solve it. The objective of the diagnostics system is to help the system administrator to detect non-operation of the security server and to offer solutions for elimination of failures.

The diagnostics system checks the security server configuration and network connection gradually and offers solutions for any detected failures. Tests can be activated automatically (all tests are run until the first failure or successful passing of all tests) or manually.

To run the diagnostics:

1. On the **System** menu, click **Diagnostics**.
2. Click **Test all** to run all tests in succession
   –or–
   Click **Run** to run a single test.

If a test fails or is canceled, the **Advise** button will be displayed next to the test. Clicking the button opens a window with possible problems with and solutions for the failure.

Regardless of the test results, the output of the test can be examined by clicking **Output**. The displayed information can be used e.g. for more thorough troubleshooting.

11.4 SWITCHING BETWEEN SHA-1 AND SHA-512

It is possible that a security server uses a version of the OpenSSL library that doesn't support the SHA-512 hash algorithm. However, using the older hash algorithm (SHA-1) can cause problems in communicating with information systems or adapter servers interfaced with the security server. As a workaround, the security server can be switched to a compatibility mode using the script *obsolete_intcert.sh*.

obsolete_intcert – shows the current value
obsolete_intcert 1 – switches to the compatibility mode (SHA-1 support)
obsolete_intcert 0 – switches to normal mode of operation (SHA-512 support)

The change takes effect immediately.

11.5 RE-HASHING OLD QUERY LOGS

Starting from version 5.0, the security server uses the SHA-512 algorithm to hash query logs, as the older, SHA-1 algorithm is considered insecure. However, as changing the hash function ensures a secure hash chain only for new log records, the hash chain created using the old algorithm needs protection against attacks as well.

Therefore, to ensure that the old query logs cannot be tampered with, the logs must be re-hashed with a new hash algorithm. For more details, refer to the document "X-Road Query Log Re-hasher. User's Guide.".

11.6 USING "XOP" MIME ATTACHMENTS

Starting from version 5.0, the security server supports the XOP style of attachments (*XML-binary Optimized Packaging)*. To use it in a message with a MIME container, set the "Content-type" parameter to "application/xop+xml".

11.7 STOPPING AND STARTING SECURITY SERVER SERVICES

For troubleshooting, it might become necessary to start or stop the following security server services, for which purpose Ubuntu has the commands *stop* and *start*. **If in doubt, consult with the system maintainer.** In all cases, enter either:

```
sudo start <service>
```

–or–

```
sudo stop <service>
```

Where <service> can be one of the following:

- xtee-adapterchecker
- xtee-asyncmanager
- xtee-consumerproxy
- xtee-datasender
- xtee-idlesender
- xtee-mangler
- xtee-netstats
- xtee-producerproxy
- xtee-sslogd

12 APPENDIX

12.1 MIB DEFINITION OF SNMP MESSAGES

Starting from version 5.0, the security server's SNMP MIB *(Management Information Base)* definitions are distributed with the server package and placed under */usr/xtee/etc/snmp_mib_definitions.txt*.

12.2 TROUBLESHOOTING.

Most problems can be resolved with the following measures.

Table 1. Possible solutions of the problems

Problem source	Possible tips and solutions
General	• Try the operation again • Enter the data again • On the **Configuration** menu, select **Reconfigure all** • Archive log files to free up disk space • Restart the system to remove temporary files
Configuration (general)	• Check the configuration; if necessary, re-enter the data • Restore the configuration from a back-up copy
Configuration locking	• Check that there are no lingering semaphors belonging to 'www-data' (list with **ipcs**, remove with **ipcrm**). Ensure that you know what you are doing!
DNS key	• Wait until the DNS key is loaded in the central server • Check the network connection • Make sure that the key comes from a trusted source • Make sure you entered the key fingerprint correctly • Contact the central server's administrator
Making or refreshing queries	• Make sure there is a correct URL in the adapter server configuration • Make sure the problem is not caused by an internal error in the adapter server
Missing default queries	• Add the queries *getCharge* and *describeMethodAsXML* manually
Initiating an SSL connection	Make sure of the following: • the security server can connect to DNS, • the security server's DNS cache is empty, • the opposite security server has a valid certificate, • the security server has a correct DNS key.
HTTPS communication with adapter server	• Make sure you have loaded the adapter server's certificate and the adapter server has loaded the security server's self-signed certificate.

12.3 ERROR MESSAGES FOR SECURITY SERVER AND IS/DATABASE INTERACTION

Table 2 presents the X-Road SOAP protocol error codes and their descriptions. The errors are sent as notifications to the system administrator.

Table 2. SOAP protocol error codes with explanations

SOAP error code	Description
Client.InvalidQuery	Invalid SOAP query (decoding error)
Server.InternalError	Internal server error. Study the logs in order to find a more specific reason.
Server.Producer.ProcessingError	Cannot process database's security server's query (possible reasons: the query was incomplete, the configuration couldn't be accessed, etc)
Server.Consumer.CannotSign	The organization's security server was unable to sign the query
Server.NoResponse	No response from the data source (i.e., database's security server or adapter server)
Server.Consumer.InvalidSignature	The response received from the database's security server did not contain a valid signature
Server.Consumer.InvalidResponse	The response received from the database's security server did not contain a valid SOAP response
Server.Consumer.CannotLog	The organization's security server was unable to correctly log the query or response
Server.Producer.CannotReceive	The organization's security server was unable to correctly receive the query
Server.Producer.InvalidSignature	The response received from the organization's security server did not contain a valid signature
Server.Producer.InvalidQuery	The response received from the organization's security server did not contain a valid SOAP query
Server.Producer.NotAllowed	The organization is not allowed to perform this query
Server.Producer.CannotListQueries	Unable to fulfill an *.allowedMethods query in the database's security server
Server.Producer.CannotSign	The database's security server was unable to sign the query
Server.Consumer.NoProducerList	Unable to get a list of databases from the central server
Server.Consumer.FormResponse	Unable to compose a SOAP response in the database's security server
Server.Producer.NoPartnerCertificate	The database's security server was unable to get the partner's certificate to verify messages
Server.Producer.InvalidFault	The adapter server issued a fault message with an invalid structure
Server.Consumer.NoDiskSpace	The organization's security server has not enough disk space to save query logs
Server.Producer.NoDiskSpace	The database's security server has not enough disk space to save query logs
Server.Producer.PeerCertificate	The organization's name in the query and the organization's name in the certificate do not match.
Server.Producer.CannotLog	The database's security server was unable to corrently log the query or response
Server.Consumer.ProcessingError	The organization's security server was unable to process the query (possible reasons: the query was incomplete, the configuration couldn't be accessed, etc)
Client.UnsupportedQuery	Unsupported or unknown query
VersionMismatch.*	Unknown error string in the SOAP message
MustUnderstand.*	
Client.*	
Server.*	