Instructions for verifying X-Road queries

Date	Version	Description	Author
12.12.2001	1.0	Initial version	Märt Laur
13.12.2001	1.01	Content-related amendments	Margus Freudenthal
14.12.2001	1.02	Linguistic corrections	Märt Laur
02.12.2005	1.1	Additions related to securing	Märt Laur
06.12.2005	1.2	Corrections	Märt Laur
28.10.2010	1.3	Additions due to re-hashing old query logs. Amended/updated the chapter dealing with installing additional software (Ubuntu support).	Kristo Heero
04.02.2011	1.4	New document template + some corrections	Alexander Andrusenko
11.02.2011	1.5	Corrected to be consistent with the code	Alexander Andrusenko

Contents

1 INTRODUCTION

1.1 EXPLANATION

Queries are performed via the X-Road system, and sometimes momentous actions are undertaken based on the responses received. Therefore it is essential that in the event of later disputes the person receiving the response could prove that the action was undertaken based on particular information obtained from a database. A database must also be capable of proving performing of unauthorised queries.

The evidence material for query verification comprises the following components.

- **The security server query log**, used to store all queries or query responses intermediated by this security server. Queries are stored on the database side, and query responses on the institution side. The log entries are linked to preceding log entries using a hash function. This allows forgery attempts to be discovered as in a forged log the entries do not form an uninterrupted chain.
- **A consolidated file obtained by re-hashing the old security server query logs, and the corresponding response file obtained from the central server.** Starting from version 5.0 the security servers use the SHA-512 algorithm for hashing their query log entries, as using the SHA-1 hash function was no longer secure. However, replacing the hash function only ensures the secure linking chain for new log entries added, and due to that also the linking chain created using the old hash function must be protected from attacks. This means that the old query logs had to be re-hashed, and the consolidated file obtained from these hashes had to be logged by the auditing server running on the central server, receiving the response file in the event of success.
- **The central server log** containing the intermediate values of all security server query logs (and the hashes of consolidated files obtained by re-hashing old query logs) This guarantees the security server administrators cannot later forge the logs.
- **The database of the certification centre** containing all certificates issued during the entire system lifetime. This allows the owner of the public key used to sign a query or query response to be ascertained.
- **Specifications** helping to interpret the queries and query responses (this document does not discuss their usage).

Query identifiers (ID) are used to identify the queries during verification. The identifiers of the queries performed are managed by the information system of the institution in question. For example, MISP displays the query identifier with the query response to the user.

Two utilities must be used to perform the operation under discussion:

- the **sqaverify** utility is used on the **security server** side (remember: S like **S**ecure);
- the **cqaverify** utility is used on the **central server** side (remember: C like **C**entral);

NB! The files moving between the central and security servers during query authenticity verification, can be distributed using secure e-mail. In that case deleting e-mail headers or other non-related text is not required before the file is loaded in the utility; keeping the BEGIN and END lines and the data between them intact is sufficient.

NB! During query authenticity verification data are transferred between the central server and security server administrators. The authenticity and integrity of these data is extremely important as they directly influence the verification result. The utilities described in this document do not offer protection against forgery of the data exchanged between the server administrators; this must be ensured with the help of other means.

1.2 INSTALLATION OF ADDITIONAL SOFTWARE

Additional software must be installed due to the need to also verify the queries secured by using the ID card authentication certificate. This software must be installed only on a special workstation in possession of the system administrator, used to run the `sqaverify` utility.

1.2.1 Installation of the ID card driver

The ID card drivers must be installed to verify queries signed with ID card authentication certificates. To do this, open the `http://www.ideelabor.ee` web site, and install the ID card drivers for Debian/Ubuntu Linux provided there.

1.2.2 Installation of the OpenSC module

The verification utility requires the **OpenSC PKCS#11** module to work. For this purpose, install the package

libengine-pkcs11-openssl.

The utility assumes the OpenSC module has been installed in the `/usr/lib/engines/` directory; this directory is also used as the default location on package installation. If the engine_pkcs11.so module file is located elsewhere, its file name with the directory path must be set using the appropriate environment variable, e. g. using the following command:

```
export ENGINE_PKCS11_PATH=/usr/local/lib/openssl/engine_pkcs11.so
```

1.2.3 Other libraries

The sqaverify and cqaverify utilities are dependent on the following packages:

- zliblg
- libqt3-mt
- libssl0.9.8
- libexpat1
- libglib2.0-0
- libice6
- libsm6
- libxml2

Depending on the workstation configuration all the required packages might not be installed by default. Issue the **`ldd cqaverify`** or **`ldd sqaverify`** command, if necessary – if a message is returned, telling that a dynamic library is missing, this library must be installed.

2 QUERY VERIFICATION

Query verification comprises three stages.

Stage **I** is performed on the security server: the query corresponding to the identifier submitted is located in the security server logs archive (if required, also the consolidated file obtained by re-hashing old query logs must be provided), and its ID, hash (and the consolidated file hash, if necessary), and the certificate hash are exported to a text file. This file is transferred to the central server.

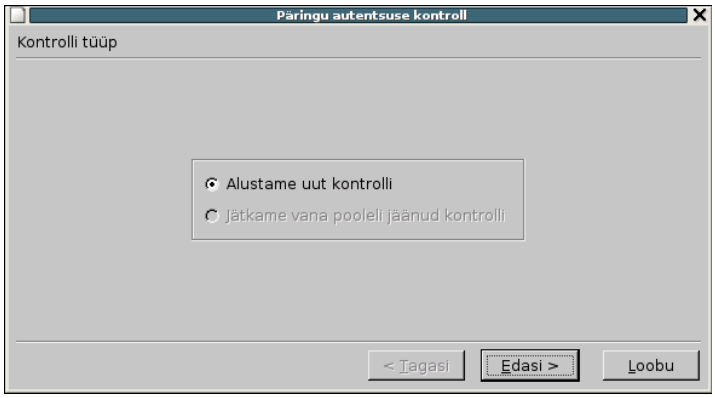
Stage **II** is performed at the X-Road centre: the text file received from the security server containing the query is loaded, and the hash (and also the consolidated file hash, if available) and certificate submitted are located in the central server's complete log hash and certificate databases, respectively. The file containing the information obtained is exported, and returned to the security server.

Stage **III** is again performed on the security server: the response from the central server is loaded, the log entry is decrypted (in case of secured log entries) and verified, and the final decision regarding the authenticity of the query is displayed.

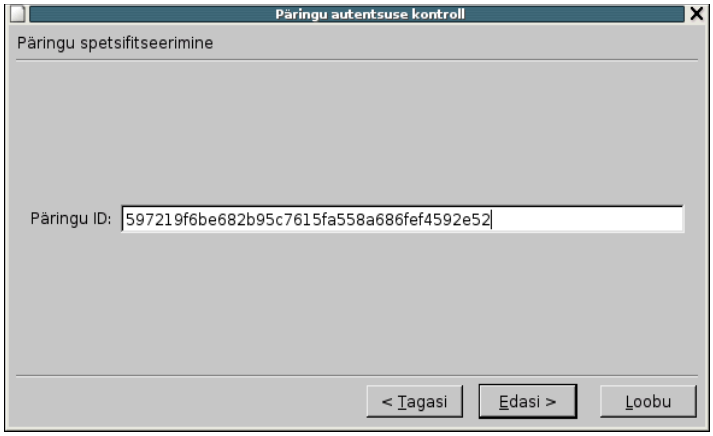
2.1 PROCEDURE I FOR THE SECURITY SERVER'S SYSTEM ADMINISTRATOR

If in your capacity as the system administrator of a security server you have been ordered to verify the authenticity of a query having a specific identifier (ID), proceed as follows.

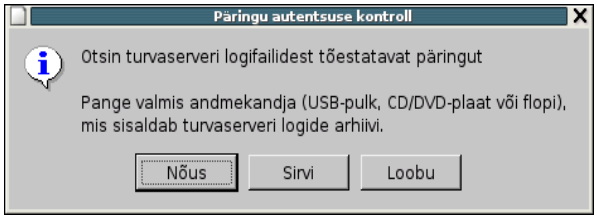
First start the `sqaverify` query verification utility.



Select *Alustame uut kontrolli* (Start new check) and click on *Edasi* (Next). Clicking on *Loobu* (Cancel) now or any time during the subsequent steps will close the utility.



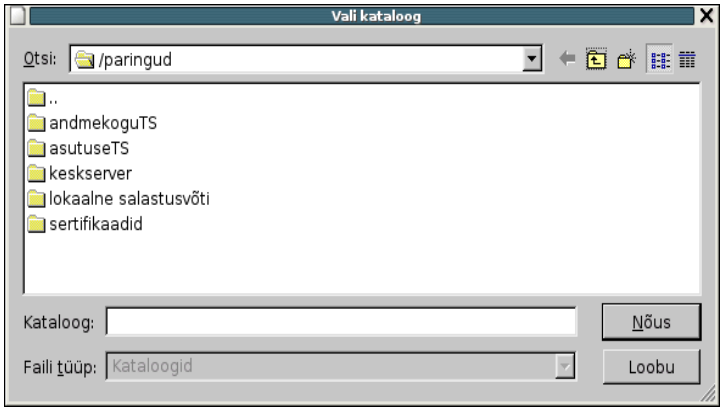
Enter the query ID in the field (it is case-sensitive, i.e. distinguishes between uppercase and lowercase letters), and click on *Edasi* (Next). A dialog appears prompting you to specify the location of the log files.



If the logs are located on a CD-ROM then insert the disc in the drive and click on *Nõus* (OK).

You can also use a DVD but in this case you must first mount it to the `/cdrom` directory using the **`mount`** utility.

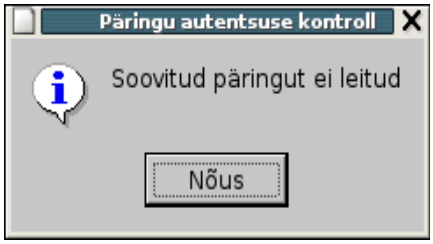
If the logs are located on your workstation's hard disk (or on a mounted device), click on *Sirvi* (Browse). The file browsing window opens.



Select the directory containing the log files and click on *Nõus* (OK). Clicking on *Loobu* (Cancel) returns you to the select loading location dialog.

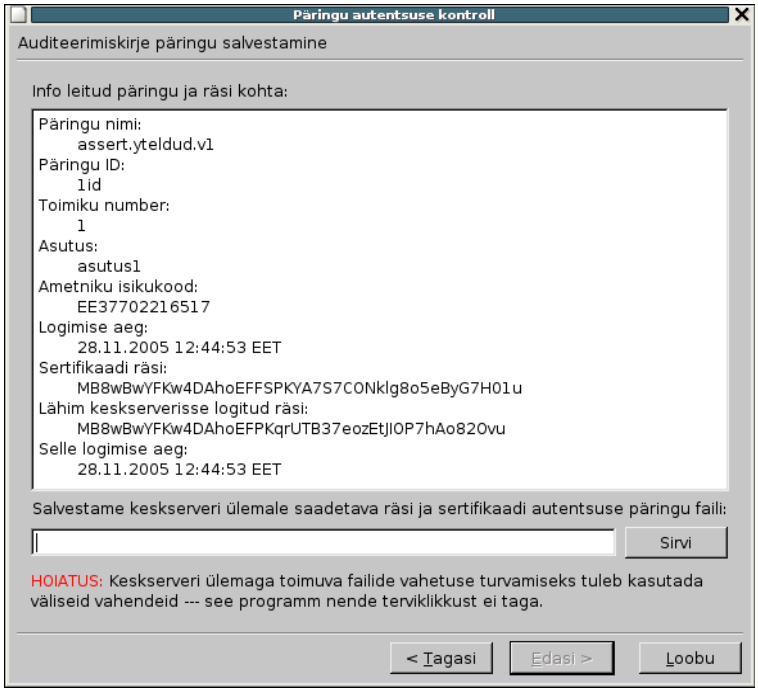
The utility starts to search the query matching the ID entered, loading the logs either from the data medium or specified location. Depending on the data transfer rate of the system and/or data medium, and the size of the archive this could take up to 15 minutes.

If the query is not found or a problem with the data occurs (e.g. the hash chain read from the disc was not consistent), an error message is displayed.



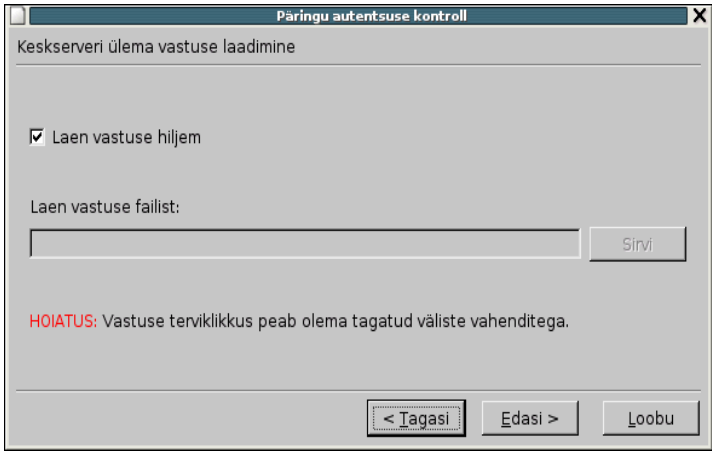
You are returned to the enter query ID window after clicking on *Nõus* (OK) in the error message window.

If the operation **succeeds** the query and hash data found are displayed (you are first prompted for the consolidated file of re-hashed query logs and the corresponding response file, if necessary).



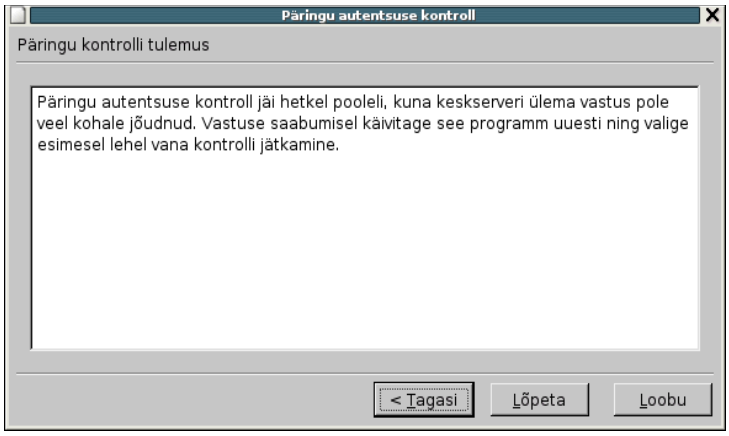
Save the result to a file. Enter the file name in the field or click the *Sirvi* (Browse) button, and specify the directory and file name, then click on *Edasi* (Next).

Next you have the opportunity to load the response from the central server.



Select the *Laen vastuse hiljem* (Load the response later) check box, as the result of the search performed on the security server must be first delivered to the central server. Click on *Edasi* (Next) to continue.

A message informing you of discontinuing the operation is displayed:



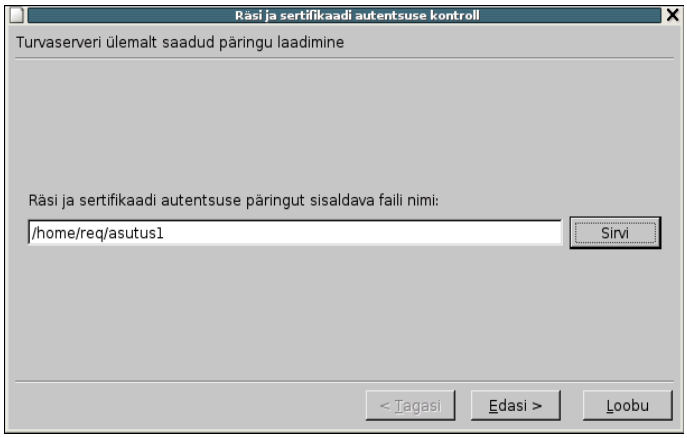
Click on *Lõpeta* (Finish). The utility is closed. NB! The verification in process is saved, so you can continue it from the same point when starting the utility next time. Click on *Loobu* (Cancel) to forgo saving the data of the current verification operation.

Then deliver the file you have just saved to the central server's system administrator using the secure method prescribed (a registered letter, PGP signed e-mail etc.). You can continue verification after receiving the response from the central server's system administrator.

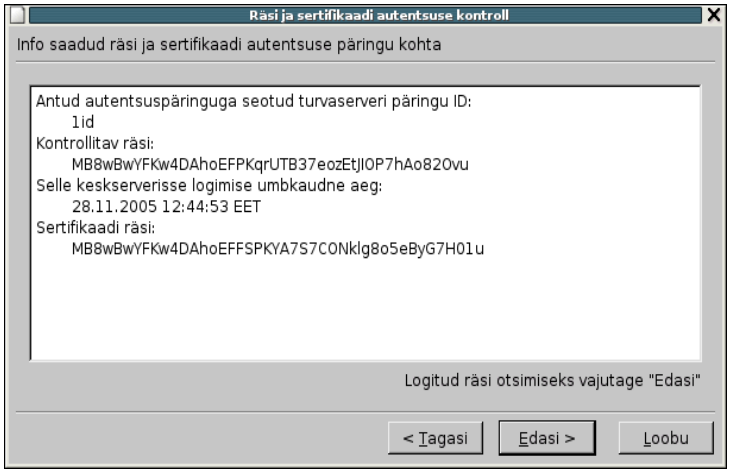
2.2 PROCEDURE FOR THE CENTRAL SERVER'S SYSTEM ADMINISTRATOR

Proceed as follows after receiving the file containing the query from the security server's system administrator.

First start the **`cqaverify`** utility.



Load the query sent from the security server. For this, click on *Sirvi* (Browse), locate the file containing the query, and click on *Ava* (Open). Then click on *Edasi* (Next). The data contained in the loaded file are displayed.



Click on *Edasi* (Next) to start the hash search. A dialog prompting you to specify the location for searching the logs archived on the central server, containing the data for the date provided in the query.

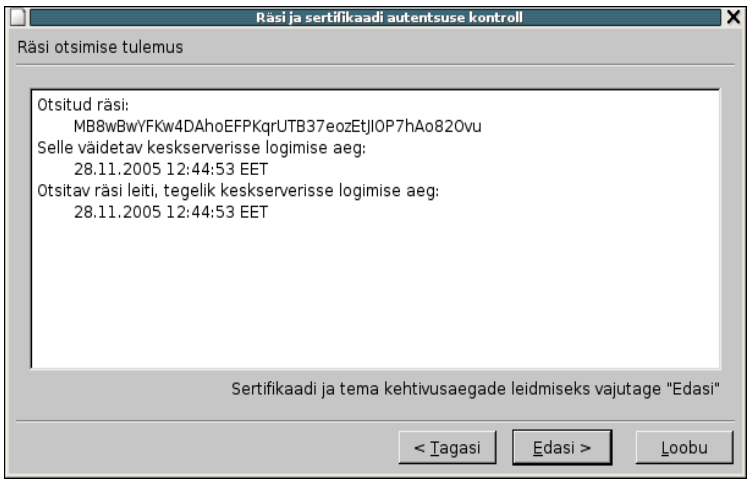
If the logs are located on your workstation's hard disk (or on a mounted device), click on *Sirvi* (Browse), and specify the location of the log files.

If the logs are located on a CD-ROM then insert the disc in the drive and click on *Nõus* (OK). You can also use a DVD but in this case you must first mount it to the `/cdrom` directory using the **`mount`** utility.

If the hash is not found on the disc inserted in the CD-ROM drive you are returned to the dialog box above. You can then insert another disc containing query logs in the drive, and try again.

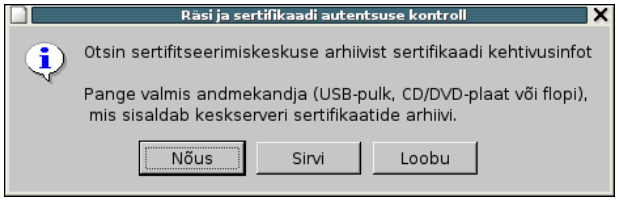
If the hash is not found the query cannot be verified. This could be either a forged query or query external to the system.

If the hash is found, an appropriate message is displayed (if the query received from the security server also contains the hash of the consolidated file of re-hashed query logs, you must also locate this in the central server logs).



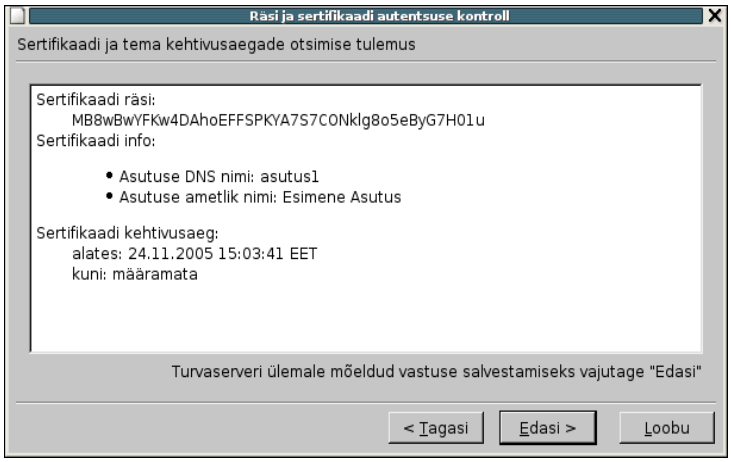
Click on *Edasi* (Next) in this window.

Next insert the archive copy of the database of certificates stored at the certification centre in the CD-ROM drive. You can use any archive, provided it has been created after the time of performing the query.

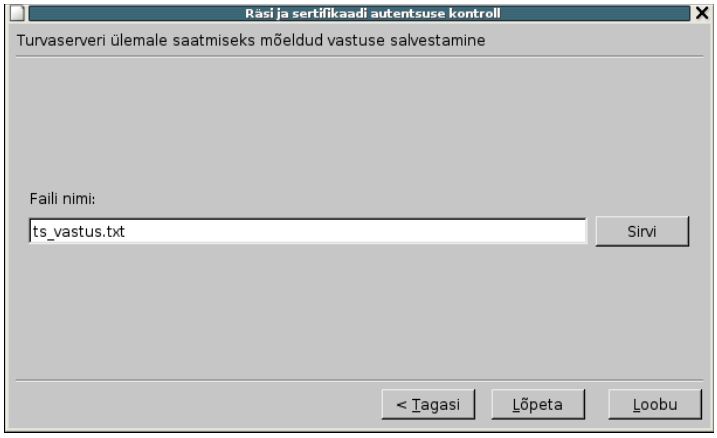


If the logs are located on your workstation's hard disk, click on *Sirvi* (Browse), and specify the location of the certificates directory. If the certificates are located on a CD-ROM then insert the disc in the drive and click on *Nõus* (OK).

If the certificate matching the hash is not found, you are returned to the previous dialog. If the certificate is found, its validity information is displayed in the window:



Click on *Edasi* (Next). The last screen is opened.



Click the *Sirvi* (Browse) button, and select the directory and file name to be used for storing the response to the security server's administrator. You can also enter the name directly in the appropriate field. Then click on *Lõpeta* (Finish).

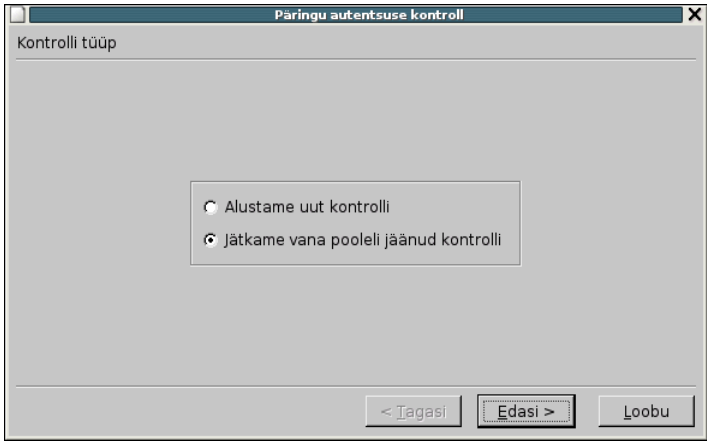
NB! Modification of this file affects the result of the query authenticity verification!

Therefore make sure the integrity and authenticity of the response is ensured when it is delivered to the security server's system administrator.

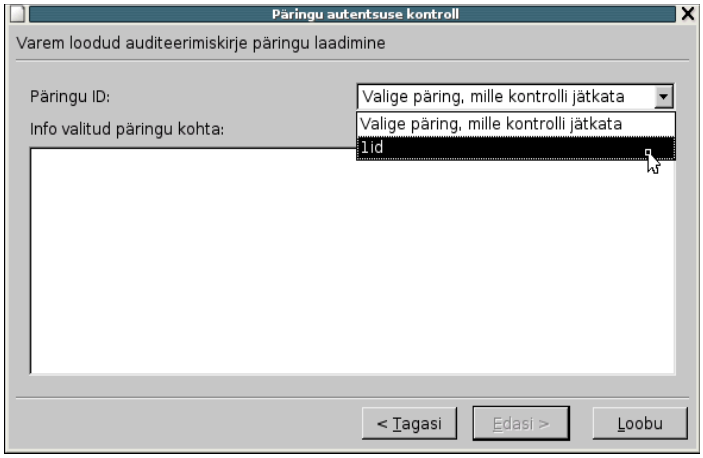
2.3 PROCEDURE II FOR THE SECURITY SERVER'S SYSTEM ADMINISTRATOR

The security server's system administrator receives a reply from the central server's administrator, and performs the following operations to complete the query authenticity verification.

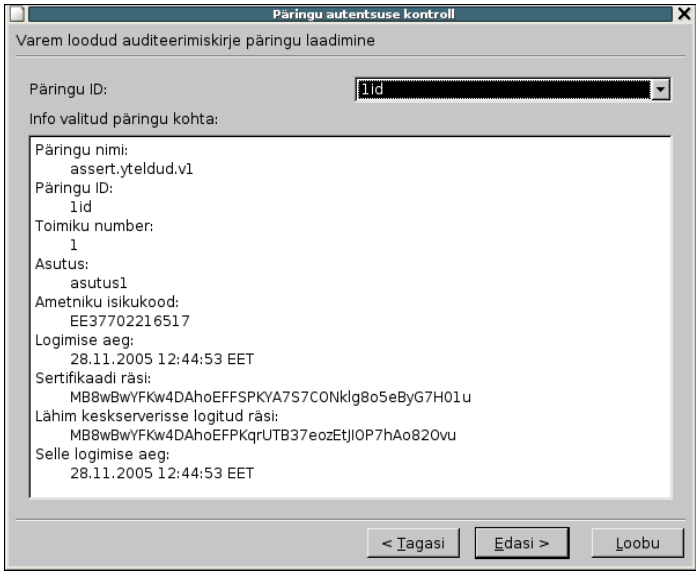
Start the **cqaverify** utility. Select the *Jätkame vana pooleli jäänud kontrolli* (Continue the verification in progress) option, then click on *Edasi* (Next).



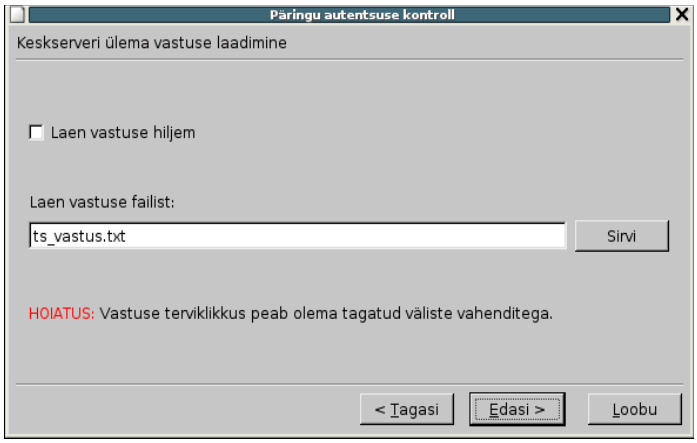
Load the response received from the central server. Analysis of this response will determine the final query verification result. Click on the drop-down list at the upper right of the window, and select the query whose verification to continue.



The data of this query are displayed after it has been selected.



Click on *Edasi* (Next). A dialog appears, enabling you to load the response from the central server's system administrator.



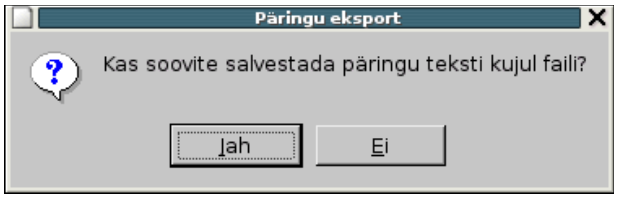
Click on the *Sirvi* (Browse) button, and specify the file containing the response. Click on *Ava* (Open) to load the file, then click on *Edasi* (Next).

Further activities depend on whether the log entries are stored as cleartext or encrypted. In the latter case you need a matching private key for decrypting the secured log entry.

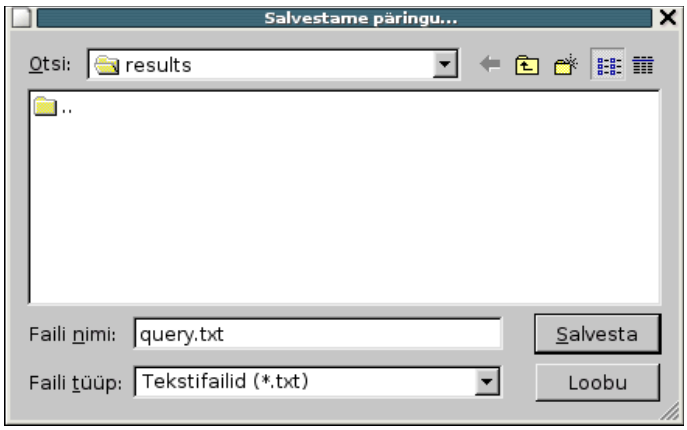
- If the log is unencrypted, the query verification result is displayed immediately. Proceed to Section 2.3.1 Unencrypted log.
- If the log has been encrypted using the local security server key, the message "*Logikirje on krüpteeritud sertifikaadiga "Turvaserveri salastamine"*" (This log entry has been encrypted using the "Secured by security server" certificate) is displayed. Proceed to Section 2.3.2 Log encrypted using the local security server key.
- If the log has been encrypted using the key of the X-Road central server, the message "*Logikirje on krüpteeritud X-tee keskuse salastussertifikaadiga* (This log entry has been encrypted using the encryption certificate of the X-Road centre) is displayed. Proceed to Section 2.3.3 Log encrypted using the encryption key of the X-Road centre.
- If the log has been encrypted using the encryption key of the ID card, the message "*Logikirje on krüpteeritud ID-kaardi autentimissertifikaadiga*" (This log entry has been encrypted using the ID card authentication certificate) is displayed. Proceed to Section 2.3.4 Log encrypted using the ID card authentication certificate.

2.3.1 Unencrypted log

The following dialog is displayed:

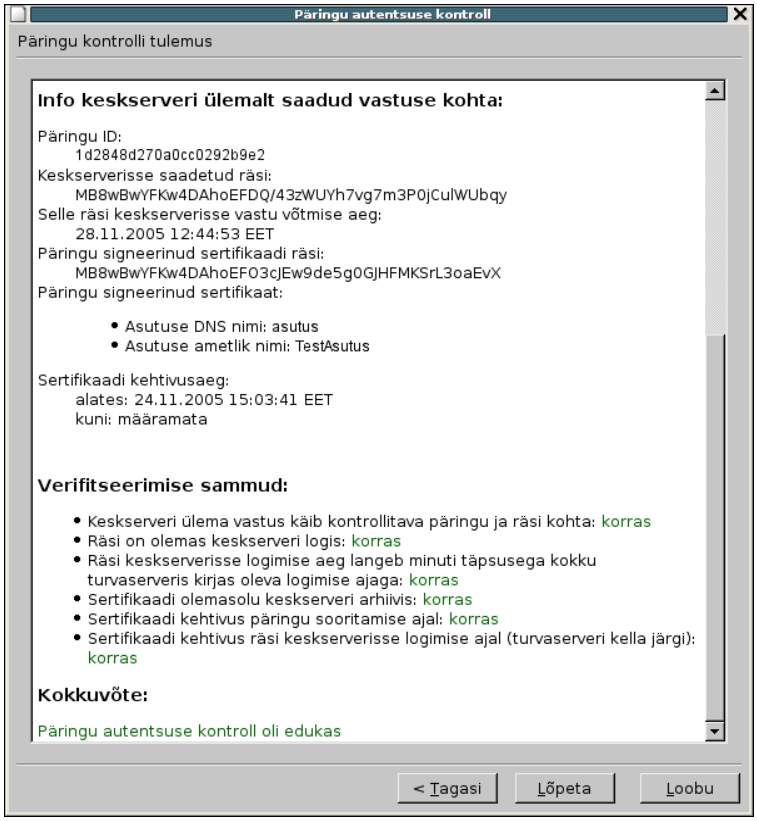


Clicking on *Jah* (Yes) opens a dialog box for saving the query. Clicking on *Ei* (No) skips this step.



If you chose to save the query, enter the file name for the query, and click on *Salvesta* (Save).

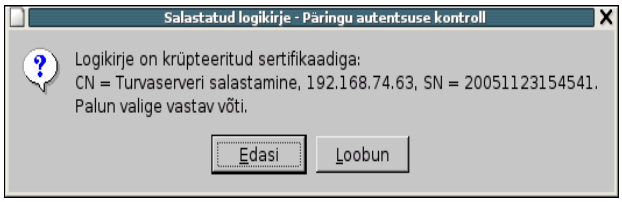
The query verification result is displayed after that:



This completes the query verification procedure. Click on *Lõpeta* (Finish) to close the utility.

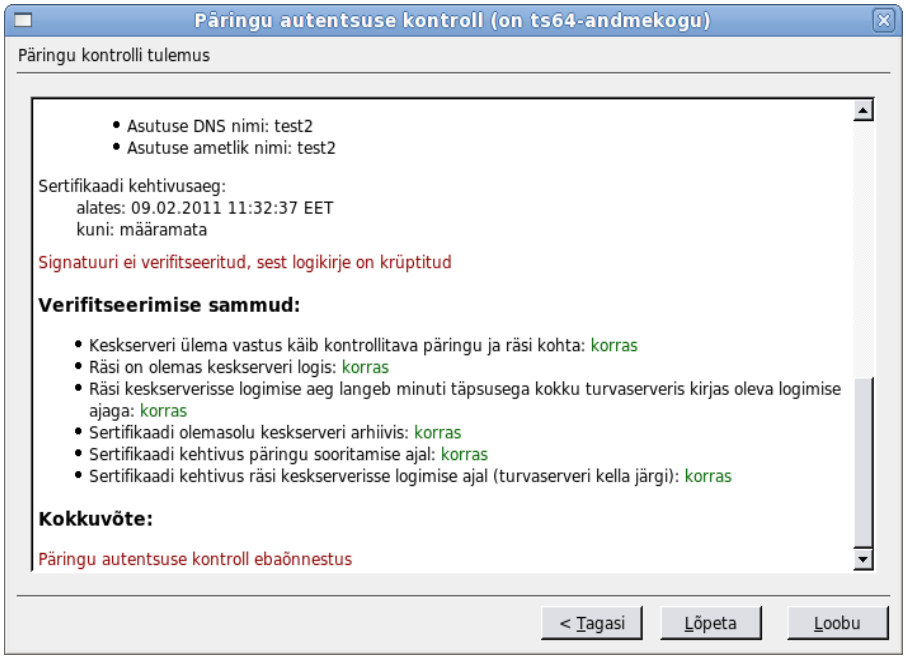
2.3.2 Log encrypted using the local security server key

If the log has been encrypted using the local security server private key, a message similar to the one provided below is displayed.

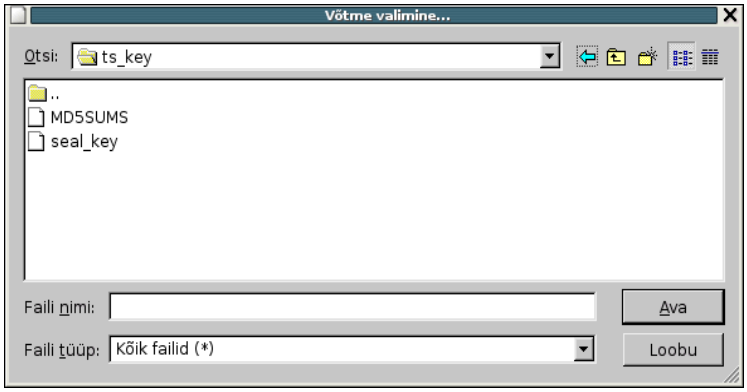


The value of the issuer parameter CN of the local security server encryption certificate is "Turvaserveri salastamine, <väline IP aadress>" (Secured by security server, <external IP address>", and the value of the serial number parameter SN is the time of issuing (generating) the certificate in the `YYYYMMDDhhmmss` format (e.g. 20050913122011). The combination of CN and SN uniquely identifies the certificate.

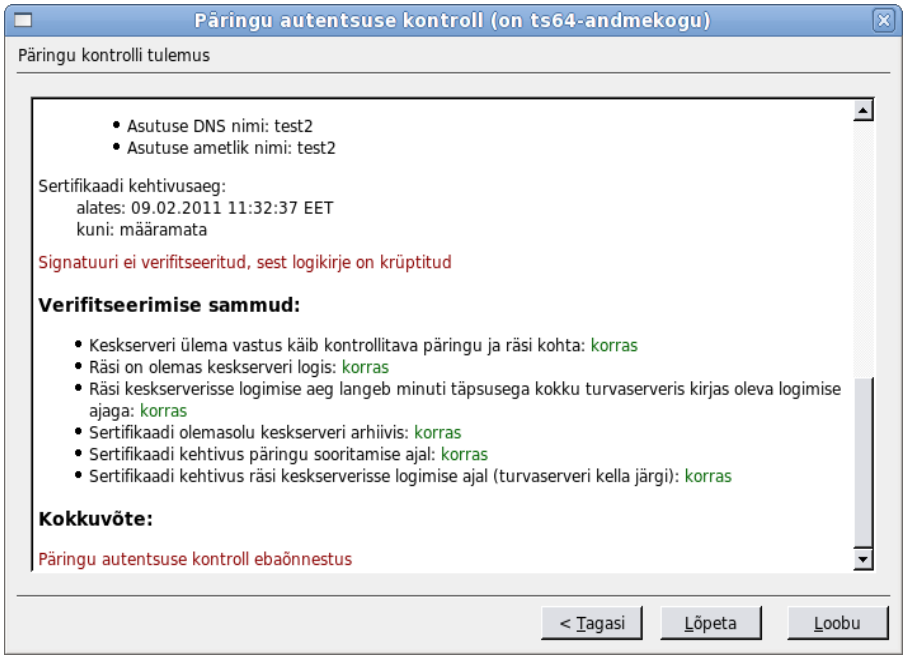
When clicking on *Loobu* (Cancel), query verification is not completed, and the query verification result is displayed instead, with the message "Signatuuri ei verifitseeritud, sest logikirje on krüptitud" (Signature was not verified as the log entry is encrypted).



Clicking on *Edasi* (Next) opens the browse dialog.



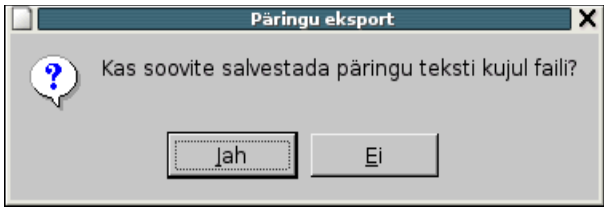
Locate the key file, and then click on *Ava* (Open). If the key is not valid (e.g. the file format is wrong or the query has not been encrypted with the selected key), an error message is displayed followed by the query verification result with the message “Päringu autentsuse kontroll ebaõnnestus” (Query authenticity verification failed).



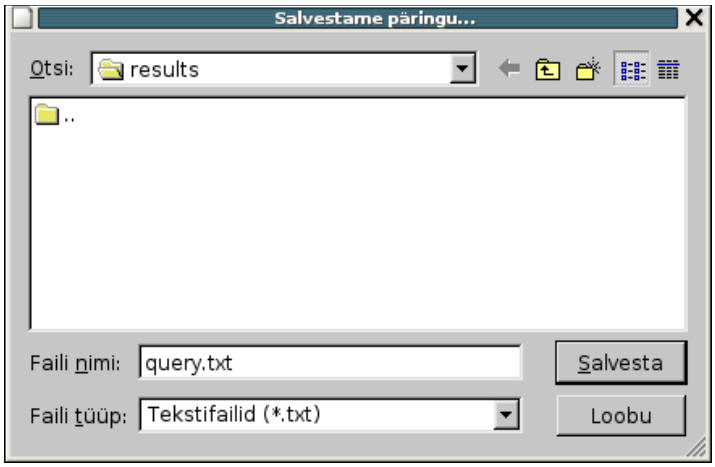
If the key you opened is valid there are two possibilities.

- The query could be doubly encrypted, if encryption with the X-Road centre's key is used in addition to local encryption. In that case a dialog prompting for the X-Road centre's key is displayed immediately after you have provided the correct local encryption key. Proceed to Section 2.3.3 Log encrypted using the secrecy key of the X-Road centre.
- If the query has been encrypted using only the local security server encryption key, proceed as described below.

The following dialog is displayed:

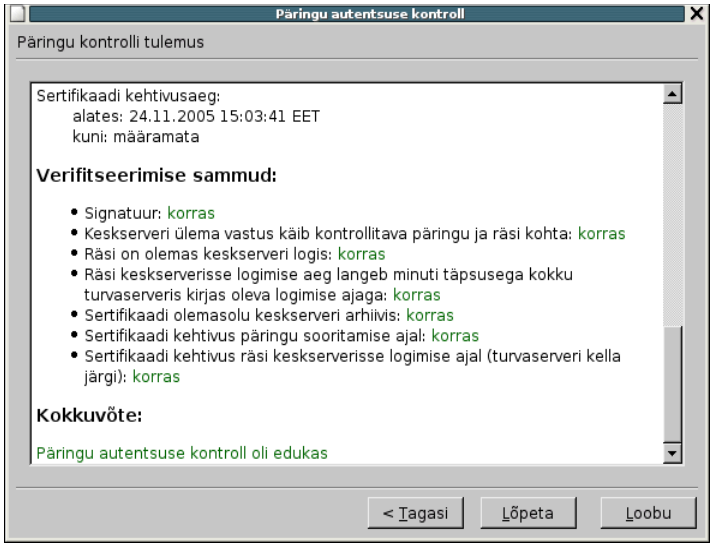


Clicking on *Jah* (Yes) opens a dialog box for saving the query. Clicking on *Ei* (No) skips this step.



If you chose to save the query, enter the file name for the decrypted query, and click on *Salvesta* (Save).

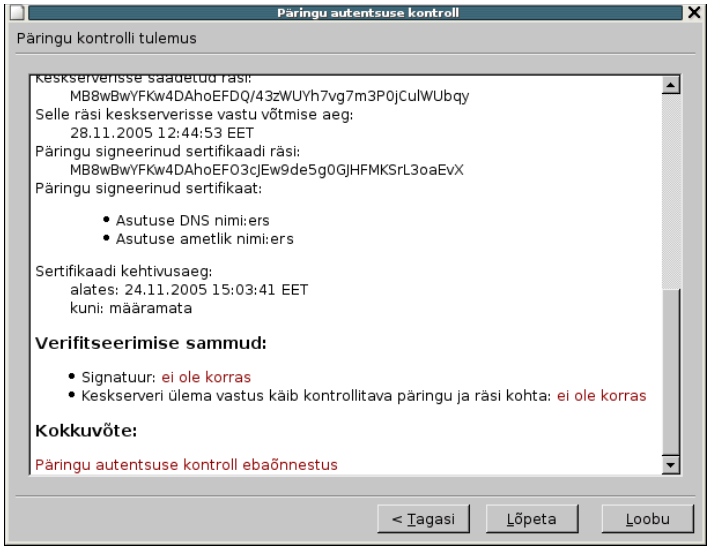
Then the query verification result is displayed. If the verification was successful an appropriate message is displayed in the information window.



If the log is unencrypted, all attachment hashes are also displayed in the information window to allow the user to check them.

The hashes are calculated over the byte sequence of the decoded attachment content (without the headers). The structure of the attachments is not processed. In case of compound type attachment contents (either *multipart* or *message*, itself containing MIME sections), the hash of the attachment body is calculated as provided in the message (no further decoding is needed thanks to MIME restrictions). If the attachment has no sub-sections, it could use either base64 or *quoted-printable* encoding that is first decoded for hashing.

If the operation fails, e.g. the central server discovers the certificate had been revoked for the time of performing the request, a respective explanation is displayed in the information window.



This completes the query verification procedure. Click on *Lõpeta* (Finish) to close the utility.

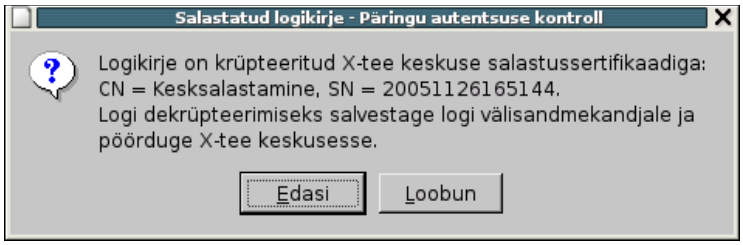
2.3.3 Log encrypted using the encryption key of the X-Road centre.

Verifying the legality of log entries of this type involves the following activities.

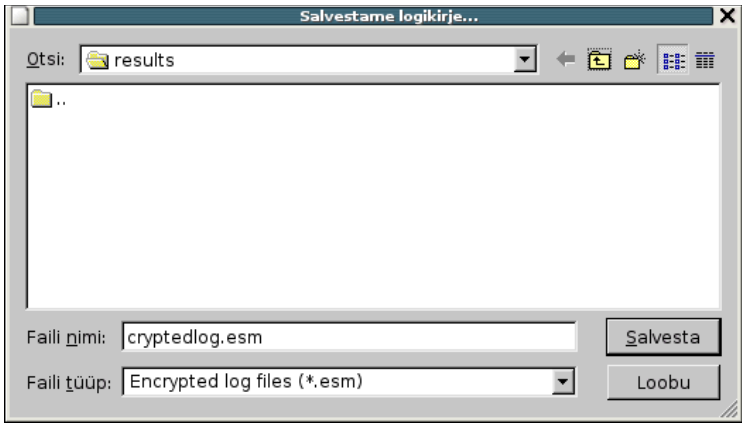
1. A regulatory body submits a request to the database, asking them to deliver certain specific encrypted log entries.
2. The database locates the desired entries using the utility described in this document, they are stored on an external data medium, and delivered to the regulatory body.
3. The regulatory body in possession of the key segments and the data medium containing the encrypted log entries, contacts the X-Road centre with the request to decrypt the log entries. Decryption is performed according to established procedures.

The value of the issuer parameter CN of the X-Road centre's encryption certificate is "Kesksalastamine" (Central securing), and the certificate is uniquely identified by the serial number parameter SN, equal to the time of issuing (generating) the certificate in the `YYYYMMDDhhmmss` format (e.g. 20050913122011).

If the log has been encrypted using the central server's encryption key, a message similar to the one provided below is displayed.

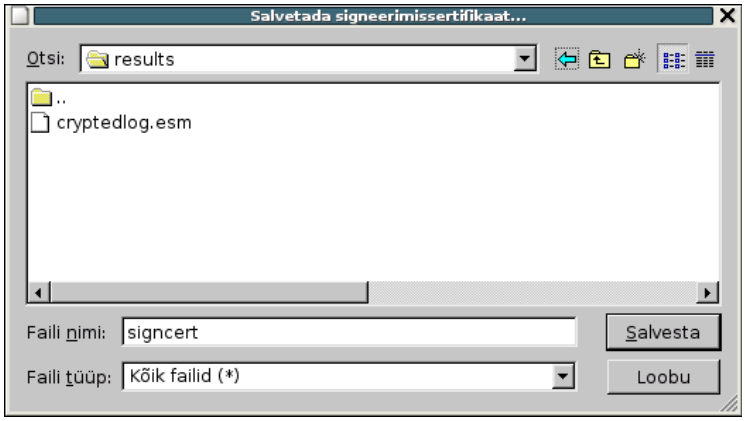


Click on *Edasi* (Next). A window appears, prompting you to specify the location for saving the `cryptedlog.esm` log entry file.



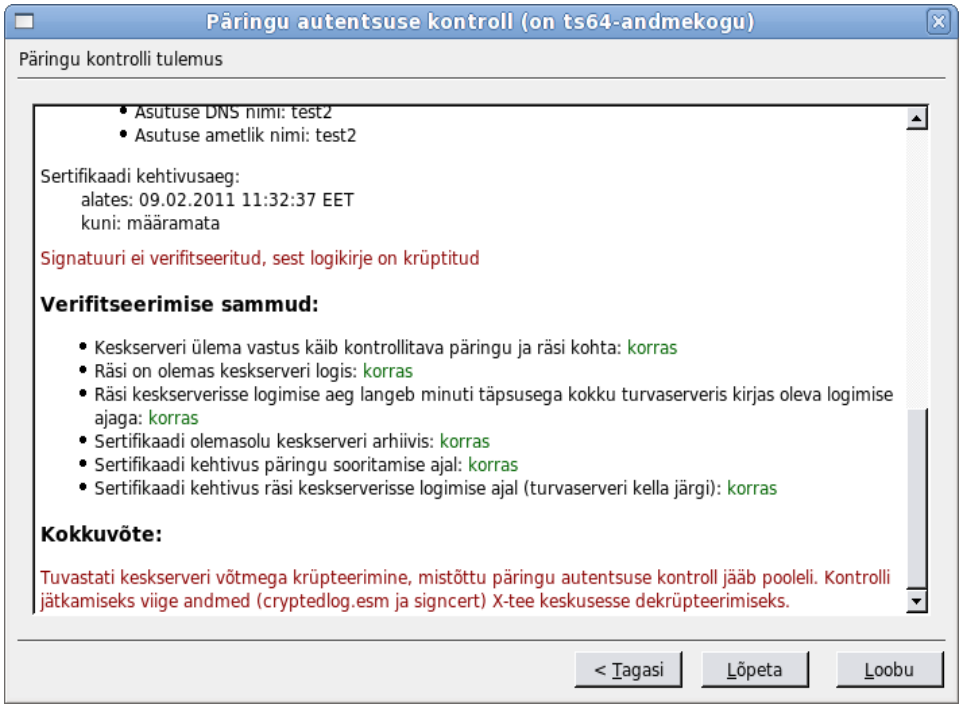
Select an appropriate directory, and click on *Salvesta* (Save). The following dialog is displayed.

Select *Jah* (Yes) to save the `signcert` file containing the signing certificate on the data medium.



Select the directory for saving the file, enter the file name, and click on *Salvesta* (Save).

Last the query verification result is displayed.



As the log entries encrypted with the X-Road encryption key cannot be decrypted on the security server, the note “Signatuuri ei verifitseeritud, sest logikirje on krüptitud” (Signature was not verified as the log entry is encrypted) is also displayed. If the log is unencrypted, all attachment hashes are also displayed in the information window to allow the user to check them.

The hashes are calculated over the byte sequence of the decoded attachment content (without the headers). The structure of the attachments is not processed. In case of compound type attachment contents (either *multipart* or *message*, itself containing MIME sections), the hash of the attachment body is calculated as provided in the message (no further decoding is needed thanks to MIME restrictions). If the attachment has no sub-sections, it could use either base64 or *quoted-printable* encoding that is first decoded for hashing.

Log entries encrypted with the encryption key of the X-Road centre can be decrypted only at the X-Road centre, via the certification server software having the correct private key for decryption in HSM. For that reason the data exported during the last step (`cryptedlog.esm` and `signcert`) must be delivered to the X-Road centre.

These data must be loaded to the certification server at the X-Road centre, and decrypted. Find the appropriate instructions in the “Decryption of encrypted query logs” section of the X-Road certification centre user manual. If the `signcert` file is present on the data medium taken to the centre, and decryption is successful, it also means succeeding with the final verification of the query log. If the file mentioned is present on the data medium but verification fails, an appropriate error message is displayed.

The decrypted log entry is stored on an external data medium on the certification server, and handed over to the representative of the regulative body.

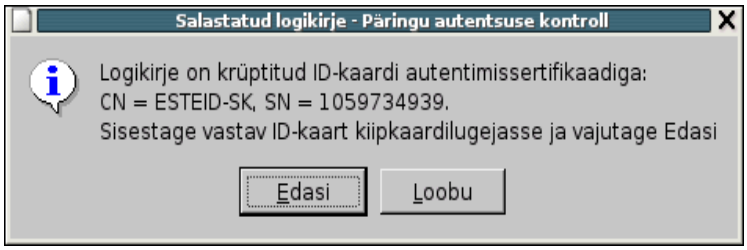
This completes the query verification procedure. Click on *Lõpeta* (Finish) to close the utility.

2.3.4 Log encrypted using the ID card authentication certificate

The key of the ID card authentication certificate is used to secure the queries of the Citizen Portal. A citizen desiring to verify a query performed must request that the query be decrypted on the institution’s security server using his/her ID card. In the event of the ID card being destroyed, replaced, or its certificates updated, the queries encrypted with the old card can no longer be decrypted.

The value of the issuer parameter CN of the ID card is “ESTEID-SK”, and the certificate is uniquely identified by the serial number parameter SN.

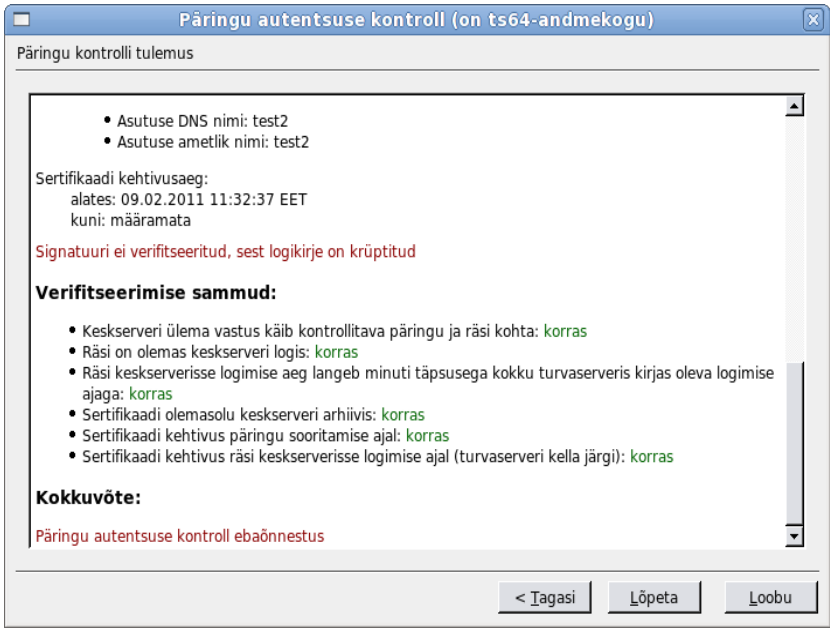
If the log entry has been encrypted with the ID card authentication certificate, a message similar to the one below is displayed:



When clicking on *Loobu* (Cancel), query verification is not completed, and the query verification result is displayed instead, with the message “Signatuuri ei verifitseeritud, sest logikirje on krüptitud” (Signature was not verified as the log entry is encrypted). This also ends the query verification process.

If discontinuing the procedure is not desired, insert the ID card with the required serial number in the reader, and click on *Edasi* (Next). A dialog opens, prompting you to enter the ID card’s PIN1 code. Enter the code and click on *Nõus* (OK).

If verifying the signature fails (i.e. no ID card was inserted or a wrong ID card was inserted), the utility will not display attachment information, and the message “Signatuuri ei verifitseeritud, sest logikirje on krüptitud” (Signature was not verified as the log entry is encrypted) is returned instead.



If the log is unencrypted, all attachment hashes are also displayed in the information window to allow the user to check them.

The hashes are calculated over the byte sequence of the decoded attachment content (without the headers). The structure of the attachments is not processed. In case of compound type attachment contents (either *multipart* or *message*, itself containing MIME sections), the hash of the attachment body is calculated as provided in the message (no further decoding is needed thanks to MIME restrictions). If the attachment has no sub-sections, it could use either base64 or *quoted-printable* encoding that is first decoded for hashing.

This completes the query verification procedure. Click on *Lõpeta* (Finish) to close the utility.