# Estfeed Adapter Administrator Manual

**Version: 1.5**
**14.07.2017**
**19 pages**
**Doc. ID: Y-1031-1**

| Date | Version | Description |
|---|---|---|
| 29.05.2016 | 0.1 | Initial |
| 10.06.2016 | 0.2 | New packages, configuration creation, TLS certificates |
| 29.06.2016 | 0.3 | Minor fixes and additions |
| 15.07.2016 | 0.4 | New software release notes |
| 19.07.2016 | 0.5 | PGP key changes |
| 02.09.2016 | 0.6 | NTP added |
| 09.09.2016 | 0.7 | Java8 package signing key added |
| 07.10.2016 | 0.8 | X-Road and IS entry point URLs added |
| 09.02.2017 | 0.9 | Updated WSDL URL |
| 06.04.2017 | 1.0 | Added chapter about troubleshooting adapter log messages |
| 25.04.2017 | 1.1 | Protocol diagram, better references to X-Road SS key management UI. |
| 27.04.2017 | 1.2 | Some adapter logging clarifications |
| 03.05.2017 | 1.3 | Section about message exchange logging |
| 28.06.2017 | 1.4 | Section about Estfeed message delivery verification |
| 14.07.2017 | 1.5 | Some improvements to the Estfeed message delivery verification |

# Table of Contents

# 1 Introduction

This document describes the installation, management and maintenance of an Estfeed adapter.

## 1.1 The Estfeed Adapter

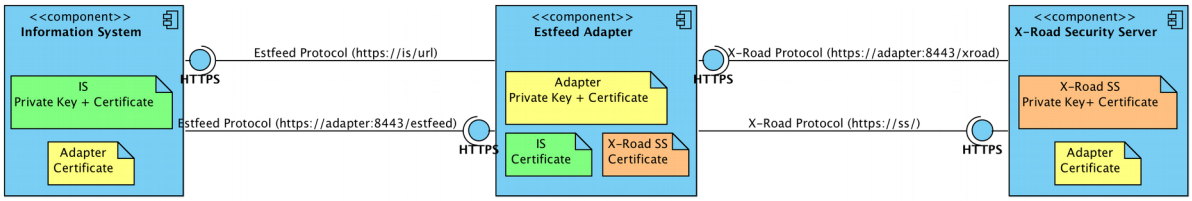


**Figure 1. Estfeed adapter in a typical installation.**

Estfeed adapter is the component that provides an interface to the Estfeed system. Each information system communicating over the Estfeed system is connected to its adapter that relays the Estfeed messages to other adapters:

- Application/Data source (information system) communicates with the adapter using Estfeed protocol secured with TLS [EF_PR].
- Adapter communicates with the X-Road security server.
- Application adapter: Receives data published by data sources from the X-Road security server and sends it to the application information system. Forwards requests from the application information system to the data source adapter servers over the X-Road based on service providers configured in the configuration.
- Data source adapter: Receives data published by the data source information system and sends data to application adapter servers over the X-Road based on subscriptions configured in the configuration. Forwards requests from the application information system received from the X-Road security servers to the data source information system.
- Adapters enforce service permissions.
- Adapters enforce mandate-based access rights to messages containing private data.
- Adapters log Estfeed traffic and private data use.

## 1.2 Terms and Abbreviations

TODO

- Application
- Data source
- X-Road security server

## 1.3 References

1. [EF_PR] Estfeed Protocol. Cybernetica AS, 2016, Y-1029-1.
2. [EF_MDV] Estfeed Message Delivery Verification. Cybernetica AS, 2016, Y-1031-6.

# 2 Release Notes

| Version | Date | Description |
|---|---|---|
| 1.2 | 10.06.2016 | New packaging, new configuration file format. Please install new instance in another server and then migrate to the new server. |
| 1.3 | 30.06.2016 | Fixes for installation, better default values |
| 1.3 | 15.07.2016 | TLS temporarily not mandatory to ease IS migration, component logs reduced |
| 1.7 | 14.10.2016 | Changed URL entry points: /xroad for incoming connections from X-Road security server (source and application adapter) and /estfeed for information systems (independent of type) |

# 3 Installation

Installation of the packages is done using distributions package management tool. The software is provided in a form of remote repository.

## 3.1 Ubuntu 14.04

Note that all the following command need to run as root, either from root login session or prefixed with `sudo`.

Ubuntu 14.04 (trusty) uses apt repositories. Estfeed packages are distributed from HTTPS URL, so first install HTTPS support for apt:

```
apt-get update
apt-get install apt-transport-https
```

Add or replace the following line into `/etc/apt/sources.list.d/estfeed.list` file:

```
deb https://repo.cyber.ee/estfeed trusty main
```

Add or replace the following line into `/etc/apt/sources.list.d/java8.list` file (only if you do not have X-Road security server already installed in the same server):

```
deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main
```

Then update the package list by running

```
apt-get update
```

If this results in an error about GPG key not available, check the correct key fingerprint from vendor and add the key from PGP keyserver (with correct fingerprint):

```
apt-key adv --keyserver keyserver.ubuntu.com --recv \
 1F4FCE426DA93DFED8A303A6DB121184208F3AA8
```

and run `apt-get update` again (this should get rid of the error). Repeat for Java8 with key fingerprint DA1A4A13543B466853BAF164EB9B1D8886F44E2A.

Next, install the desired package and its dependencies. Depending on what adapter you are installing, run either

```
apt-get install estfeed-application-adapter
```

or

```
apt-get install estfeed-source-adapter
```

and make sure the installation succeeds with no errors.

If the server has direct access to the Internet, NTP time synchronization should work out of the box. If the server does not have direct access to the Internet, please edit `/etc/ntp.conf` and configure at least 2 accessibele NTP servers.

## 3.2 Initial Configuration

One installation of the adapter package can support multiple instances of adapters. For each adapter, a configuration must be created. Out of the box no adapters are configured

so at least one adapter configuration needs to be created for the package to be useful. This configuration consists of a configuration file, TLS key and selfsigned certificate, automated startup script and command line parameters file.

For clarity, it is recommended to name the adapters the same that X-Road subsystems are named.

To create a new configuration, run the command, replacing *myadapte*r with your adapter name:

`estfeed-add-adapter myadapter`

This command creates the needed files from a template and generates a TLS key and a certificate. The certificate generation is interactive, meaning it asks for the certificate subject fields (country, organization, organization unit, fully-qualified domain name). The following files and directories are created:

`/etc/estfeed/myadapter/`

`/etc/estfeed/myadapter/adapter.conf`

`/etc/init/estfeed-adapter-myadapter.conf`

`/etc/default/estfeed-adapter-myadapter`

`/etc/estfeed/myadapter/tls/`

`/etc/estfeed/myadapter/tls/tls-key.pem`

`/etc/estfeed/myadapter/tls/tls-cert.pem`

`/etc/estfeed/myadapter/tls/trusted-is/`

`/etc/estfeed/myadapter/tls/trusted-xroad/`

Of these, `/etc/estfeed/myadapter/adapter.conf` is the main configuration file of the adapter instance and `/etc/default/estfeed-adapter-myadapter` is the defaults file for specifying alternate command line options for the Java VM and the adapter. These files can be freely modified later.

You can customize the initial adapter settings from the command line, specifying some of the following command line options to `estfeed-add-adapter`:

| | |
|---|---|
| -f | force creating the adapter by overwriting existing configuration |
| -p port | HTTP port for local connections (default 8080, needs to be different for each adapter) |
| -s port | HTTPS port (default 8443, needs to be different for each adapter) |
| -i URL | information system URL (HTTPS URL of the information system service) |
| -x URL | X-Road security server URL (HTTPS URL of the security server) |
| -a | force adapter to be application adapter (default for estfeed-application-adapter package) |
| -r | force adapter to be source adapter (default for estfeed-source-adapter package) |
| -h | show help about these options |

If you do not provide -i and -x, you have to edit the configuration file later to add them. You should also review any other settings in the configuration file, especially data in `adapter-`

`xroad-identifier` section and `adminapp-xroad-identifier` section.

Next, please copy the trusted X-road security server certificate to `/etc/estfeed/myadapter/tls/trusted-xroad/` directory and copy the trusted information system certificate PEM files to `/etc/estfeed/myadapter/tls/trusted-is/` directory.

There can be multiple files in these directories.

The X-road security server's certificate can be obtained from the X-road security server UI:

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

Next, please start the adapter by running

```
start estfeed-adapter-myadapter
```

This will happen automatically on server startup in the future. But on first run, please read the log files under `/var/log/estfeed/myadapter.log` and `/var/log/upstart/estfeed-adapter-myadapter.log` to see if the startup succeeded, and reconfigure and restart the service until you get it working.

Once you have the adapter working, you should configure connectivity to the adapter in X-Road Security server. For that to work, you should:

1. On the Configuration menu, select Security Server Clients. Add a client for this adapter as new subsystem and preferably name it the same as you named the adapter in estfeed configuration.
2. Register the subsystem with central server.
3. In Security Server Clients, edit the corresponding subsystem and under Services, add WSDL with URL http://estfeed.ee/wsdl/estfeedData.wsdl.
4. In Security Server Clients, edit the corresponding subsystem and under Services click open the WSDL, select estfeedData and edit the service. Enter service URL https://youradapter:8443/xroad.
5. In Security Server Clients, edit the corresponding subsystem and under Service Clients, add access to this adapter to required partners.

Next, configure the information system behind the adapter:

1. Please distribute the generated TLS certificate `/etc/estfeed/myadapter/tls/tls-cert.pem` to the information system server (procedure depends on information system software).
2. Please configure the URL to adapter as https://youradapter:8443/estfeed.

Repeat the process for other adapters that must run from the same server.

# 4 Management

## 4.1 Adapter Management

To add more adapters, you can use the `estfeed-add-adapter` program described in intial setup instructions.

To remove existing adapters, you can use

`estfeed-remove-adapter` *`myadapter`*

where *`myadapter`* is the name of your adapter. This stops the adapter if it is running, removes all configurarion files and directories for this adapter and also deletes its log files from `/var/log/estfeed`.

When purging the adapter package, all configured adapters are also removed automatically.

## 4.2 TLS Key and Certificate Management

Estfeed adapters use TLS with mutual authentication for connections with the X-Road security server and the application/data source information system. Peer certificate validation is done by certificate pinning and requires the peer certificate to be saved in the system prior to setting up the TLS connection.

### 4.2.1 Adapter's TLS Key and Certificate

Adapter uses the same TLS key for connections with both the X-Road security server and with the application/data source information system.

By default, the TLS key of the adapter is stored in the file

```
/etc/estfeed/<adapter.name>/tls/tls-key.pem
```

and the TLS certificate of the adapter is stored in the file

```
/etc/estfeed/<adapter.name>/tls/tls-cert.pem
```

To generate a new TLS key and certificate for the adapter, act as follows.

3. Run the script `estfeed-create-tlscert` in a private directory

   ```
   estfeed-create-tlscert -k mynewkey.pem -o mynewcert.pem [-d days]
   ```

4. Distribute the generated TLS certificate to the peer system administrators:
   - the X-Road security server administrator and
   - the application/data source administrator.

   **NB!** Do not proceed with the following steps until the peer system administrators have confirmed, that they have configured their systems to accept the new certificate. If you are also the security server administrator, upload the certificate to the security server (ADD button on “Internal servers” tab of the correct subsystem).

5. Copy or move the new key and certificate files to `/etc/estfeed/<adapter.name>/tls/`

directory.

6. Configure the adapter to use the new TLS key by editing the adapter configuration file located at `/etc/estfeed/myadapter/adapter.conf` as follows.
   a) Change the `https-connector` attribute `tls-certificate` file name value to the file name of the certificate generated in step 1.
   b) Change the `https-connector` attribute `tls-key` file name value to the file name of the key generated in step 1.
7. Restart the adapter:

   ```
   restart estfeed-adapter-myadapter
   ```

8. Read the log under `/var/log/estfeed/adapter.name.log` and test the connectivity with IS and X-Road. If everything is working, delete the previously used TLS key and certificate files.

### 4.2.2 X-Road Security Server's TLS Certificate

By default, the TLS certificate of the X-Road security server should be located in the directory

```
/etc/estfeed/<adapter.name>/tls/trusted_xroad/
```

The adapter verifies the security server's TLS certificate received during the TLS handshake against the certificates found in this directory.

To add a security server's TLS certificate, place the certificate received from the security server administrator to this directory. If you are also the security server administrator, the key can be downloaded from the SS user interface (EXPORT button on “Internal servers” tab of the correct subsystem).

To remove a security server's TLS certificate, delete the certificate from this directory.

### 4.2.3 Application/Data Source Information System's TLS Certificate

TLS is optional for `localhost` connections. For any other hosts, TLS is mandatory and therefor HTTPS needs to be used.

By default, the TLS certificate of the information system server should be located in the directory

```
/etc/estfeed/<adapter.name>/tls/trusted-is/
```

The adapter verifies the information system's TLS certificate received during the TLS handshake against the certificates found in this directory.

To add an information system's TLS certificate, place the certificate received from the information system administrator to this directory.

To remove an information system's TLS certificate, delete the certificate from this directory.

# 5 Estfeed Message Delivery Verification

## 5.1 Overview

Information system might want to verify that their Estfeed message was sent to X-Road at any given point of time. To do this, information system must keep records of the Estfeed message (or the SHA-512 hex-encoded hashes of the Estfeed message parts) sent to the adapter along with the transaction ID received in the acknowledgement response message from the adapter.

## 5.2 Prerequisites

In order for the information system to verify Estfeed message delivery to X-Road, the information system must provide the following to the adapter administrator:

1. the complete Estfeed message sent to the adapter or SHA-512 hex-encoded hashes of the Estfeed message parts;
2. the transaction ID of the Estfeed message obtained from the acknowledgement response from the adapter.

The adapter administrator also needs:

1. the X-Road message ID corresponding to the Estfeed message transaction ID. The X-Road message ID can be obtained from the administrator of the Estfeed administration application;
2. the X-Road ASIC-container corresponding to the X-Road message ID. See 5.4.1 for how to obtain the ASIC-container;
3. the ASIC-container verification configuration. See 5.4.2 for how to obtain the verification configuration.

## 5.3 Verification

Please see [EF_MDV].

## 5.4 Obtaining the X-Road ASIC-container

The X-Road ASIC-container is located either in the X-Road security server, in case the security server has not yet archived the message log, or in the log server, if the security server has archived the message log.

### 5.4.1 Downloading the X-Road ASIC-container from the security server

The ASIC-container can be downloaded from the security server using cURL, for example:

```
curl -k --cert-type pem --cert <CERT> --key <KEY> "https://<_SS_URL_>/asic?
```

```
queryId=<QUERY_ID>&xRoadInstance=<_XINST_>&memberClass=<_XCLASS_>&memberCode=<_XREG_>&subsystemCode=<_NAME_>&requestOnly&force" > asic.zip
```

where:

- <CERT> is the TLS certificate adapter uses to communicate with the security server, see chapter 4.2.1 for more information;
- <KEY> is the TLS key adapter uses to communicate with the security server, see chapter 4.2.1 for more information;
- <_SS_URL_> is the address of the security server;
- <QUERY_ID> is the X-Road message ID;
- <_XINST_> is the X-Road instance identifier of the information system;
- <_XCLASS_> is the X-Road member class of the information system;
- <_XREG_> is the X-Road member code of the information system;
- <_NAME_> is the X-Road member subsystem code of the information system;

The downloaded file is a ZIP file, which must be extracted to obtain the .asice container file.

The X-Road identifier values can be found in the adapter configuration file:

```
xroad {
  // Specifies the X-Road client identifier for this adapter.
  adapter-xroad-identifier {

    // X-Road instance.
    instance = _XINST_

    // X-Road member class.
    member-class = _XCLASS_

    // X-Road member code.
    member-code = _XREG_

    // X-Road subsystem code.
    subsystem = _NAME_
  }
  ...
  security-server-address = "_SS_URL_"
}
```

For example, command can be run in adapter server:

```
curl -k --cert-type pem --cert /etc/estfeed/src/tls/tls-cert.pem --key /etc/estfeed/src/tls/tls-key.pem "https://security-server/asic?queryId=b9e12c56-cf45-47d0-8e3e-8a6e3336d110&xRoadInstance=XX&memberClass=YYY&memberCode=ZZZ&subsystemCode=FOO&requestOnly&force" > asic.zip
```

### 5.4.2 Downloading the X-Road ASIC-container verification configuration from the security server

The ASIC-container verification configuration can be downloaded from the security server using cURL, for example:

```
curl http://<SS_ADDRESS>/verificationconf > verificationconf.zip
```

where <SS_ADDRESS> is the address of the security server.

The downloaded file is a ZIP file, which must be extracted to to a new directory.

# 6 Adapter Logging Troubleshooting

This chapter describes how to understand log messages that are logged in adapters during message exchange.

## 6.1 Log Format

Adapter logs to two files simultaneously:

- info log – contains INFO and ERROR level log entries, request metadata information and contextual information. Suitable for monitoring and troubleshooting most situations;
- debug log – contains detailed and technical log entries of all log levels. Suitable for debugging concrete situations.

The following sections in this chapter will focus on troubleshooting the adapter info log.

An entry in the info log contains the following tab-seprated fields (metadata):

- timestamp in UTC;
- adapter X-Road identifier (<INSTANCE>:<MEMBER_CLASS>:<MEMBER_CODE>:<SUBSYSTEM_CODE>);
- log level – INFO or ERROR;
- log entry type (optional) – REQUEST and SESSION are used for log entries related adapter message processing;
- transaction id (optional) – request transaction id. Only present for log entries related to request/response message processing. Useful for correlating log entries of a REQUEST;
- logging class name;
- message.

En example log entry in the INFO log reads as follows:

```
2017-04-05T09:28:33.474Z        EE:ENT:11111111:app     INFO    REQUEST 31bf54f7-
6ff6-47ba-a275-1724a06624dc    e.c.e.a.a.ApplicationRequestResponseController
Request (Test.v1 (Test)) received from application IS
```

An entry in the debug log contains the following fields:

- timestamp in UTC;
- logging thread name;
- log level;
- logging class name;
- message.

For clarity, the metadata has been omitted in the following sections and examples.

## 6.2 Application Adapter Logging

### 6.2.1 Application IS Sends Request Message: Successful Scenario

The following relevant INFO messages (correlated by transaction id) are logged:

```
Request (<service id>) received from application IS
```

and

```
Acknowledgement (<service id>) sent to application IS
```

and (for each data source providing the service)

```
Sent request (<service id>) to data source adapter <X-Road identifier>
```

and (for each data source providing the service)

```
Acknowledgement (<service id>) received from data source <X-Road identifier>
```

### 6.2.2 Application IS Sends Request Message: Message Processing Error

Various errors can occur in the application adapter during the processing of a request message from the information system.

Generally, the application adapter logs the following ERROR message whenever an error (exception) occurs during the processing of application request:

```
Message sending failure
```

followed by the stack trace.

If an error occurs during the sending of the request to X-Road, the following ERROR message is logged:

```
Error sending X-Road message to data source adapter <X-Road identifier>
```

followed by the stack trace (usually containing more detailed information about the cause of the error).

If data source or data source adapter responds with an Error message, the following ERROR message is logged:

```
Error received from data source <X-Road identifier>: <message>
```

### 6.2.3 Data Source IS Publishes Data Message: Successful Scenario

When data source publishes data message, the following INFO messages are logged:

```
Data (<service id>) received from data source <X-Road identifier>
```

and

```
Data (<service id>) sent to application IS
```

and

```
Acknowledgement (<service id>) sent to data source adapter <X-Road
identifier>
```

### 6.2.4 Data Source IS Publishes Error Message

When data source publishes an error message as response to a request, the following ERROR and INFO messages are logged:

```
Error sent to application IS
```

and

```
Acknowledgement (<service id>) sent to data source adapter <X-Road
identifier>
```

## 6.3 Source Adapter Logging

### 6.3.1 Application IS Sends Request Message: Successul Scenario

The following INFO messages are logged:

```
Request (<service id>) received from application
```

and

```
Request (<service id>) sent to data source IS
```

and

```
Acknowledgement (<service id>) received from data source IS
```

### 6.3.2 Application IS Sends Request Message: Message Processing Error

When an error occurs during the processing of the request from the application information system, the following ERROR message is logged:

```
Error during application request
```

followed by the stack trace.

### 6.3.3 Data Source IS Publishes Data Message: Successul Scenario

When data source information system publishes data, the following INFO messages are logged:

```
Data (<service id>) received from data source IS
```

and

```
Acknowledgement (<service id>) sent to data source IS
```

and (for each application subscribed to receive the data)

```
Data (<service id>) sent to application adapter <X-Road identifier>
```

and (for each application subscribed to receive the data)

```
Acknowledgement (<service id>) received from application adapter <X-Road
identifier>
```

### 6.3.4 Data Source IS Publishes Data Message: Message Processing Error

When there is an error processing the message, the following ERROR message is logged:

```
Error processing data source message
```

followed by the stack trace containing further details of the error:

- if an error is returned from X-Road:

  ```
  Received SOAP fault from application adapter <X-Road identifier>: <message>
  ```

- if an error is returned from the application information system or application adapter:

  ```
  Received error from application adapter <X-Road identifier>: <message>
  ```

If an error occurs during sending of the data to X-Road, the following message is logged:

```
Error sending X-Road message to application adapter <X-Road identifier>
```

### 6.3.5 Data Source IS Publishes Error Message

When data source information system publishes an error message, the following INFO messages are logged:

```
Received error message: <message>
```

and

```
Error message sent to application adapter <X-Road identifier>
```

## 6.4 Message Exchange Logging in Adapters

It is possible to log all incoming and outgoing Estfeed and X-Road messages to the adapter debug log. To enable logging of messages, the following configuration options must be enabled in the adapter configuration file (located at `/etc/estfeed/myadapter/adapter.conf`):

```
system-properties {
  estfeed.protocol.log-enabled = true // enables protocol level logging
  estfeed.protocol.log-messages = true // enables logging of messages
}
```

**NB!** These options should only be used for cases where it is necessary to debug a specific situation. These options should be disabled otherwise as they produce a lot of log output and log the whole message potentially containing personal data.