



|  |
| --- |
| X-Road: Central Server Architecture  **Technical Specification** |
| Version: 2.1  21.10.2015  12 pages  Doc. ID: ARC-CS |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 02.06.2015 | 0.1 | Initial version | Ilja Kromonov |
| 02.07.2015 | 0.2 | Comments and editorial changes | Margus Freudenthal |
| 03.07.2015 | 0.3 | Component diagram updated; configuration generation sequence and simple deployment diagrams added | Ilja Kromonov |
| 09.07.2015 | 0.4 | Minor fixes; Data model reference | Ilja Kromonov |
| 27.08.2015 | 0.5 | Section on high availability added | Marju Ignatjeva |
| 10.09.2015 | 0.6 | Format and captions of figures edited | Marju Ignatjeva |
| 10.09.2015 | 0.7 | Technology matrix added; editorial changes | Ilja Kromonov |
| 15.09.2015 | 0.8 | Audit log added | Kristo Heero |
| 16.09.2015 | 0.9 | Incorporated feedback from Vitali | Margus Freudenthal |
| 16.09.2015 | 1.0 | Editorial changes made | Imbi Nõgisto |
| 16.09.2015 | 1.1 | Postgres new number | Margus Freudenthal |
| 17.09.2015 | 2.0 | Editorial changes made | Imbi Nõgisto |
| 21.10.2015 | 2.1 | SSCD and password store related information added | Ilja Kromonov |

Table of Contents

[1 Introduction 5](#_Toc433272083)

[1.1 Overview 5](#_Toc433272084)

[1.2 Terms and Abbreviations 5](#_Toc433272085)

[1.3 References 5](#_Toc433272086)

[2 Component View 6](#_Toc433272087)

[2.1 Web Server 6](#_Toc433272088)

[2.2 Management Services 6](#_Toc433272089)

[2.3 Signer 7](#_Toc433272090)

[2.4 Database 7](#_Toc433272091)

[2.5 User Interface 7](#_Toc433272092)

[2.6 Servlet Engine 7](#_Toc433272093)

[2.7 Password Store 7](#_Toc433272094)

[2.8 SSCD 7](#_Toc433272095)

[3 Interfaces 8](#_Toc433272096)

[3.1 Management Services 8](#_Toc433272097)

[3.2 Download Configuration 8](#_Toc433272098)

[4 Configuration Creation Workflow 9](#_Toc433272099)

[5 Technology Matrix 11](#_Toc433272100)

[6 Deployment View 12](#_Toc433272101)

[6.1 Simple Deployment 12](#_Toc433272102)

[6.2 Deployment in High Availability Setup 12](#_Toc433272103)

License

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

# Introduction

This document describes the architecture of the X-Road central server. For more information about X-Road and the role of the central server see [ARC-G ].

This document presents an overview of the components of the central server and the interfaces between these components. It is aimed at technical readers who want to acquire an overview of inner workings of the central server.

## Overview

The central server manages the database of X-Road members and security servers. In addition, the central server contains the security policy of the X-Road instance. The security policy consists of the following items:

* list of trusted certification authorities,
* list of trusted time-stamping authorities,
* tunable parameters such as maximum allowed lifetime of an OCSP response.

Both the member database and the security policy are made available to the security servers via HTTP protocol (see Section 3.2 ). This distributed set of data forms the global configuration.

In addition to configuration distribution, the central server provides interface for performing management tasks such as adding and removing security server clients. These tasks are invoked from the user interface of the security servers. The management services are implemented as standard X-Road services and are offered via the central security server. See Section 3.1 for details.

## Terms and Abbreviations

HSM Hardware Security Module

OCSP On-line Certificate Status Protocol

RPC Remote Procedure Call

## References

ARC-G Cybernetica AS. X-Road Architecture.

DM-CS Cybernetica AS. X-Road: Central Server Configuration.

PR-GCONF Cybernetica AS. X-Road: Protocol for Downloading Configuration.

PR-MANAGE Cybernetica AS. X-Road: Management Services Protocol.

PR-MESS Cybernetica AS. X-Road: Profile of Messages.

PR-MSERV Cybernetica AS. X-Road: Management Services Protocol.

SPEC-AL Cybernetica AS. X-Road: Audit log events.

PKCS11 Cryptographic Token Interface Standard. RSA Laboratories, PKCS#11.

# Component View

Figure 1 shows the main components and interfaces of the X-Road central server. The components and the interfaces are described in detail in the following sections.

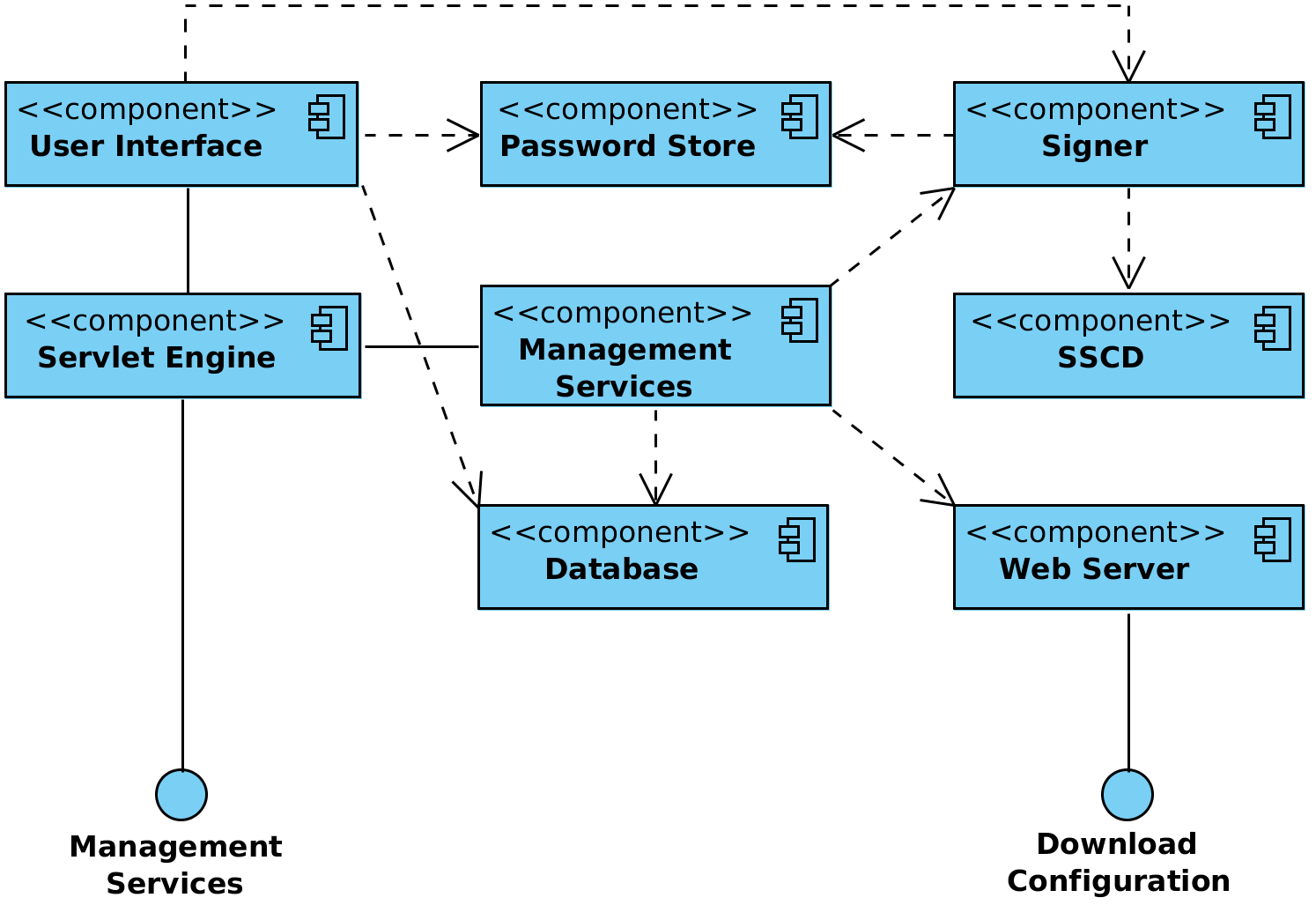


Figure 1. Components and interfaces of the X-Road central server

## Web Server

The global configuration files generated by the central server need to be made available to configuration clients. The HTTP-based protocol used for downloading configuration is described in [PR-GCONF ]. Technically, the configuration consists of a set of files that are shared out using standard web server (nginx[[1]](#footnote-1) web server is used). The global configuration generation is handled by the management services component.

## Management Services

A collection of services including:

* management services that are used by security servers to perform management tasks such as registering a security server client or deleting an authentication certificate;
* internal service for generating the global configuration.

The configuration generation service (periodically invoked by a cron[[2]](#footnote-2) job) prepares and signs the global configuration files and then copies them to the web server's distribution directory where they are distributed via standard means. See Section 4 for details on configuration distribution.

## Signer

The signer component is responsible for managing the keys and certificates used for signing the global configuration. The signer is called from the management services component to create the signature for the configuration.

## Database

The central server holds the X-Road configuration in a PostgreSQL[[3]](#footnote-3) database. The database contains the security policy of the X-Road instance as well as a list of members, security servers, global groups and management services. For a detailed description of the central server configuration refer to [DM-CS]. The configuration can be modified through the central server user interface and management services.

## User Interface

The central server user interface allows a user to manage X-Road members and security servers and define the global configuration parameters that are distributed to the security servers.

User action events that change the system state or configuration are logged into the audit log. The actions are logged regardless of whether the outcome was a success or a failure. The complete list of the audit log events is described in [SPEC-AL].

## Servlet Engine

The Jetty[[4]](#footnote-4) servlet engine hosts the user interface and management services, listening on ports that are configurable in the X-Road configuration files.

## Password Store

Stores security token passwords in a shared memory segment of the operating system that can be accessed by the central server interface and signer. Allows security token logins to persist, until the central server is restarted, without compromising the passwords.

## SSCD

The SSCD (Secure Signature Creation Device) is an optional hardware component that provides secure cryptographic signature creation capability to the signer.

The SSCD needs to be a PKCS #11 (see [PKCS11]) compliant hardware device that can be optionally used by the central server for signing the generated global configuration files it generates. The use of the interface requires that a PKCS #11 compliant device driver is installed and configured in the central server system.

# Interfaces

## Management Services

Management services are called by security servers to perform management tasks such as registering a security server client or deleting an authentication certificate.

The management service interface is a synchronous RPC-style interface provided by the central server. The service is called by security servers.

The interface is described in more detail in [ARC-G , PR-MSERV].

## Download Configuration

Configuration clients download the generated global configuration files from the central server.

The configuration download interface is a synchronous interface provided by the central server. It is used by configuration clients such as security servers and configuration proxies.

The interface is described in more detail in [ARC-G , PR-GCONF ].

# Configuration Creation Workflow

X-Road central server periodically assembles the global configuration, consisting of XML files describing private and shared parameters, as well as any additional configuration parts installed by add-ons (see [PR-GCONF ] for detailed information about configuration structure).

Configuration files are distributed in accordance with the protocol for downloading configuration (see Section 3.2 ). MIME messages are generated to represent internal and external configuration directories of the X-Road instance.

The central server implements two configuration sources. The internal source distributes files to security servers belonging to the same X-Road instance as the central server. The external source distributes configuration files to security servers of other federated X-Road instances. Both sources can contain different set of configuration files, depending on the central server's configuration.

The process of generating and distributing the configuration is the same for both configuration sources.

1. A cron job sends a request to generate the global configuration files.
2. The contents of the files are taken from central server's database. The files are saved to a temporary location.
3. Management services component generates configuration directory referencing the generated files.
4. Management services component sends a signing request (containing hash of the directory) to the signer component. Signer signs the hash and responds with the signature.
5. Management services component updates the configuration directory to contain the received signature.
6. Management services component moves the configuration files to the distribution directory of the web server.
7. Security servers make HTTP requests and download the configuration.

This process is illustrated in the sequence diagram in Figure 2.

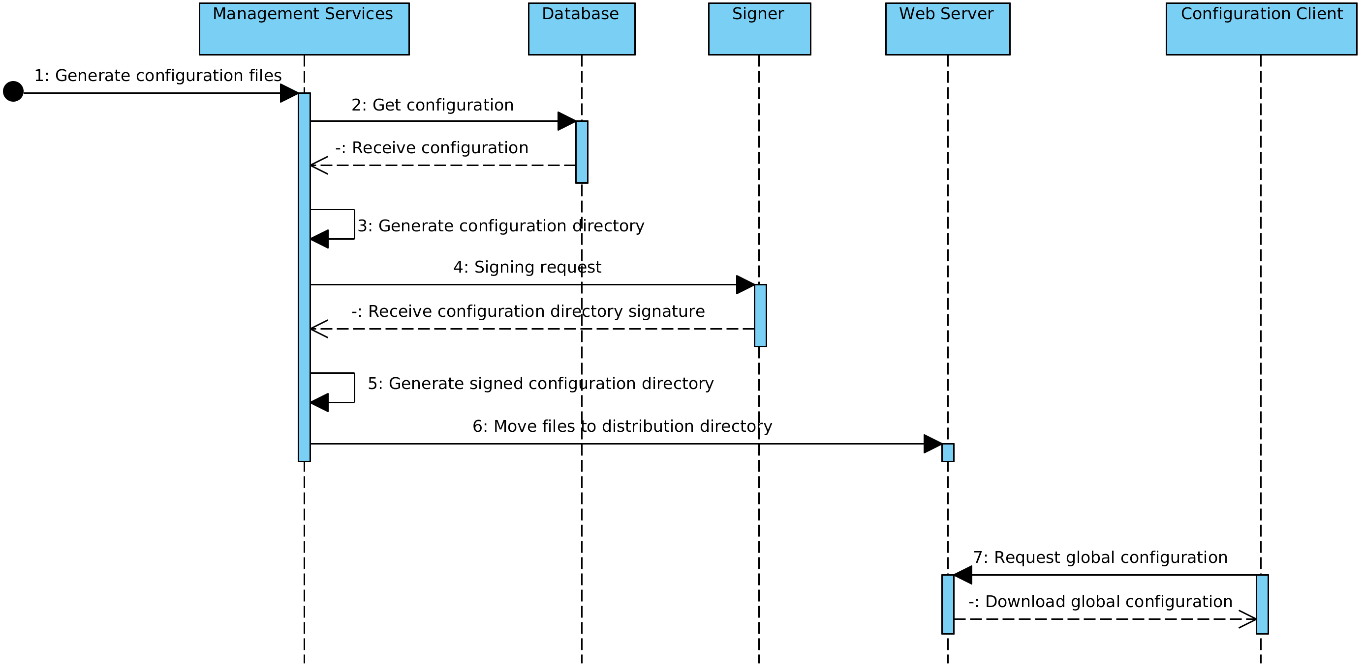


Figure 2. The process of global configuration generation and distribution

# Technology Matrix

Table 1 presents the list of technologies used in the security server and the mapping between technologies and central server components.

Table 1. Technology matrix of the central server

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Technology** | **Signer** | **Web Server** | **Password Store** | **Management Services** | **Database** | **User Interface** | **Servlet Engine** |
| Java 8 | X |  |  | X |  | X | X |
| С |  |  | X |  |  |  |  |
| Logback | X |  |  | X |  | X |  |
| Akka 2.X | X |  |  | X |  | X |  |
| Jetty 9 |  |  |  |  |  |  | X |
| JRuby 1.7 |  |  |  |  |  | X |  |
| Javascript |  |  |  |  |  | X |  |
| PostgreSQL 9.3 |  |  |  |  | X |  |  |
| PostgreSQL 9.4 |  |  |  |  | X[[5]](#footnote-5) |  |  |
| nginx |  | X |  |  |  |  |  |
| PAM |  |  |  |  |  |  | X |
| Liquibase |  |  |  |  | X |  |  |
| upstart | X | X |  |  |  |  | X |
| PKCS #11[[6]](#footnote-6) | X |  |  |  |  |  |  |

# Deployment View

## Simple Deployment

This section describes a simple scenario where the central server is installed on a standalone server without the use of redundancy. The signing key is stored on a HSM device. This setup is useful for testing environments and for X-Road instances where availability is not of critical concern.

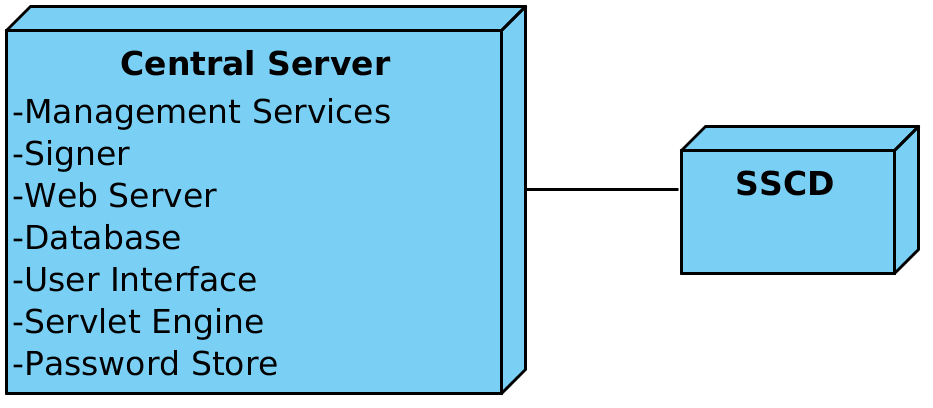


Figure 3. Simple deployment of the central server

Optionally, an SSCD can be connected with the central server if global configuration signatures are to be provided by a cryptographic hardware device.

## Deployment in High Availability Setup

This section describes the deployment of the central server in a cluster, for achieving high availability.

In the context of the central server, high availability means there exist two or more independent installations of the central server, the databases of which have been configured to form a cluster and are replicated asynchronously. The central servers (or *nodes*) share and instance identifier but have different IP addresses / hostnames, use different keys for signing the configuration, and generally do not depend on the other nodes of the cluster being available for serving users.

Asynchronous replication of the databases has been implemented using the BDR extension of the PostgreSQL database[[7]](#footnote-7).

Because data are replicated asynchronously, data modification conflicts are possible between the nodes if two users modify the same row of a table (almost) in parallel. In such cases, the default conflict resolution mechanism of BDR is used, where the latest modification of a given row will be taken into account.

In a high availability setup, the configuration clients can use any of the nodes for downloading configuration. It is up to the client implementations to choose the algorithm for selecting this node at each particular download attempt.

1. See <http://nginx.org/> for details. [↑](#footnote-ref-1)
2. See <http://pubs.opengroup.org/onlinepubs/9699919799/utilities/crontab.html> for details. [↑](#footnote-ref-2)
3. See <http://www.postgresql.org/> for details. [↑](#footnote-ref-3)
4. See <http://www.eclipse.org/jetty/> for details. [↑](#footnote-ref-4)
5. PostgreSQL 9.4 is used in High-Availability setup of the central server. [↑](#footnote-ref-5)
6. The use of cryptographic hardware devices requires that a PKCS #11 compliant device driver is installed and configured in the system. [↑](#footnote-ref-6)
7. See <http://2ndquadrant.com/en/resources/bdr/> for details. [↑](#footnote-ref-7)