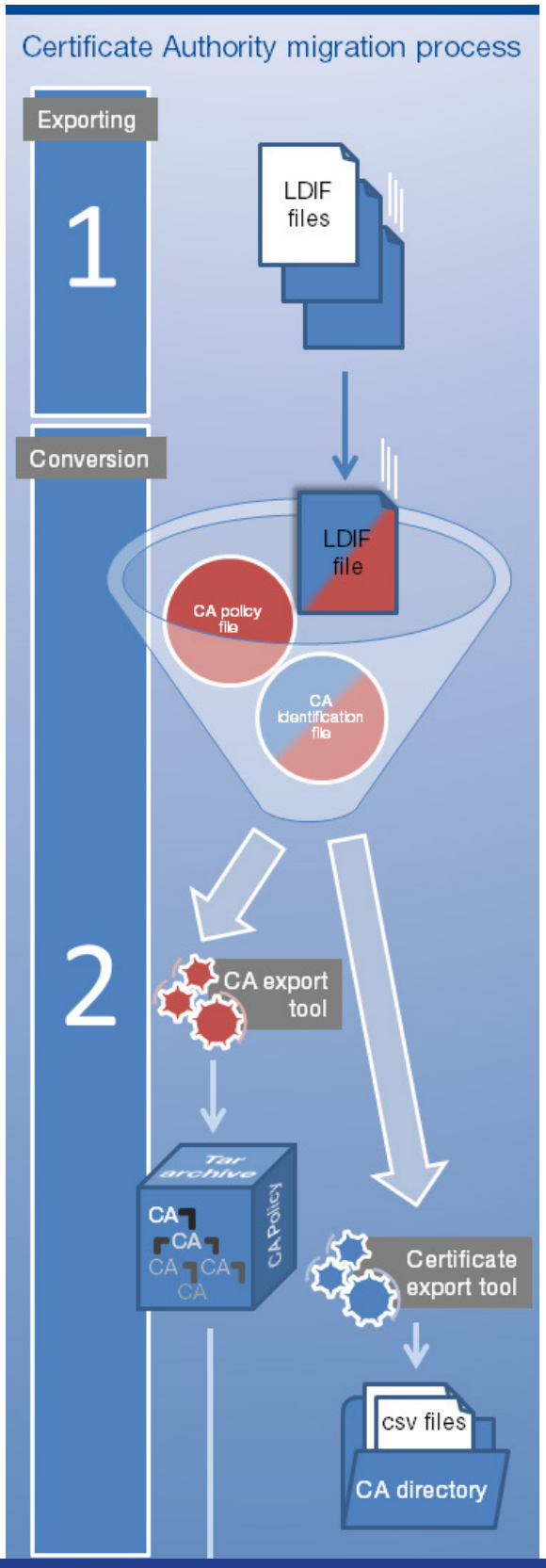
INSTA
DefSec

# Migrating from an existing CA implementation to Insta Certifier

White Paper

# Migrating from an existing CA implementation to Insta Certifier

Insta Certifier is a flexible, standards based CA (Certificate Authority) product for security-critical enterprises requiring a CA solution with long lifecycle. This White paper provides an overview of the migration process to enable successful transition from an existing CA implementation to Insta Certifier. RSA Keon CA is used here as an example but the process is similar for migration from other CA implementations as well. For more information, please contact support@insta.fi.




## What is migration?

Migration is a process of moving data used in an old system to a new system. Typically, the need for migration is caused by an end-of-life situation or substantial benefits provided by the replacing system. The migration process includes transferring data from one systems database to another. During the process, it may be necessary to convert data from the old system to an importable format.

In a typical CA migration, a large amount of data related to digital certificates needs to be processed while maintaining data integrity. Migration process speed, reliability and ease of use are crucial factors when importing millions of certificates into an online system with high availability requirements.

## The 5 steps to successful CA migration

### 1. Exporting data from the old system

First, existing data needs to be exported from the RSA Keon database for further processing. The data is exported to LDIF files (a file presentation of LDAP directory) with RSA Keon's export functionality. These files contain the Certificate and Certificate Authority (CA) data used in the old system.

### 2. Converting data for Insta Certifier CA

Next, the LDIF files are converted to a format supported by Insta Certifier CA. In some migration projects, only specific CAs may need to be imported into the new system. To enable this, a list of CAs to be imported can be provided. It is also possible to change or modify CA policies (certificate issuance rules per CA) during the conversion phase.

## 2.1 Converting CA data and setting up policies

Certificate Authority export tool reads CA hierarchies from Keon LDIF file and converts them to Certifier format. CAs to be converted can be defined with a CA identification file. In addition, CA policies in a CA hierarchy tree can be modified with a CA policy file. Once the conversion is complete, the tool outputs a .tar CA archive file as well as a report about the conversion process.

## 2.2 Converting end entity certificates

Certificate export tool reads certificate data from Keon LDIF file and converts it to Certifier format. Each .csv file contains certificates issued by one CA. As with CAs, it is possible to choose certificates from all or just specific issuers (CAs) to be converted. Once the conversion is completed, the issuer specific .csv files are ready to be imported.

## 3. Importing data into the new system

Once the conversion phase is completed, all necessary data needs to be imported correctly into Insta Certifier database. Import tools connect directly to the database checking the existing database for duplicates and ensuring data integrity. Insta Certifier is stopped automatically for the duration of the import process to prevent conflicts in data.

## 3.1 Importing CAs

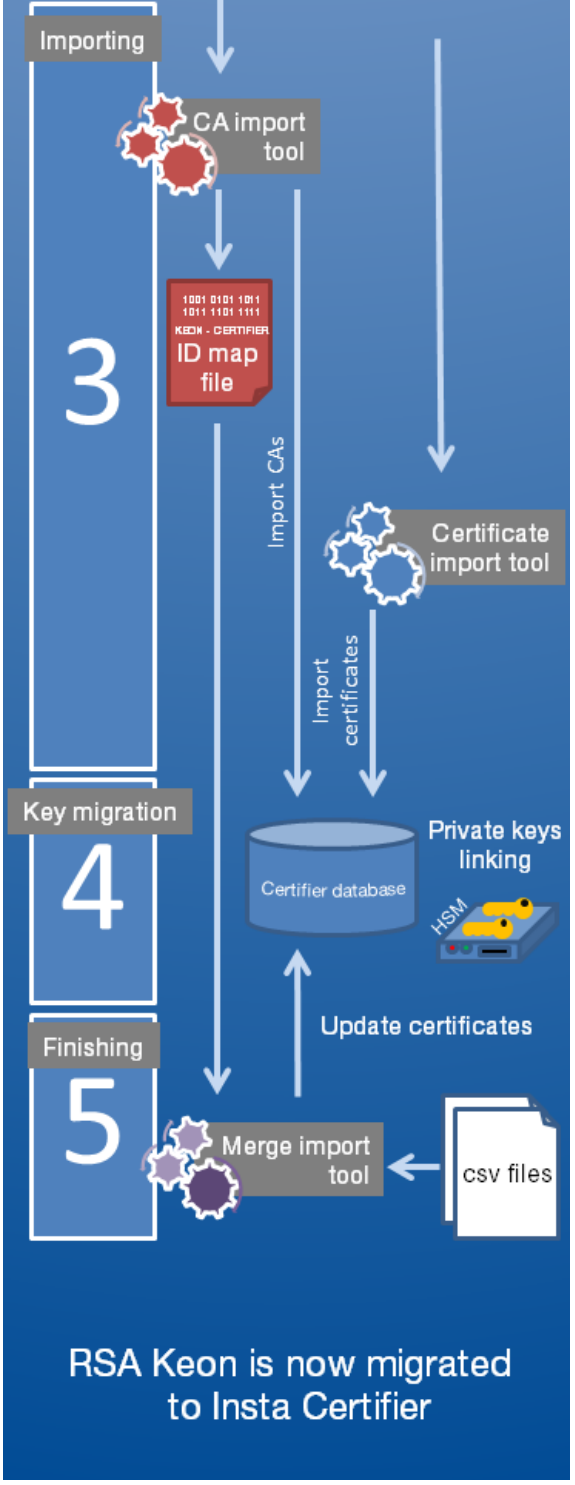
Certificate Authority import tool imports CA data from .tar archives into Insta Certifier database. To allow modifications later, a CA ID map file with CA relationships between the old RSA Keon system and Insta Certifier will also be created.

## 3.2 Importing end entity certificates

Certificate import tool imports certificates from .csv files into Insta Certifier database. The tool automatically links certificates with their issuer CA previously imported.

## 4. Key material migration

Once all CA information has been imported into Insta Certifier database, keys stored in Hardware Security Module (HSM) need to be retargeted. Insta Certifier uses keys through PKCS#11 interface, and the key migration is carried out with the HSM vendor's retarget tools. After retargeting, the keys are linked to corresponding CAs with Insta Certifier administrator UI.




## 5. Finishing the migration process

If the old RSA Keon system was brought offline when migration was started, there are no additional steps required at this point, and the migration is ready. However, since a massive data migration may take a considerable time, the old system is usually kept online during the migration to enable usage of the CA. During the migration, some data - e.g. certificates - could have been added or status updated, and this delta data needs to be updated to Insta Certifier database before the old RSA Keon system can be shut down.

Merge import tool is used to import this delta data between the originally exported data and the latest status of the old RSA Keon systems database. The process is similar to the certificate import process described earlier, except that the old operational system must be brought offline after the last delta import to avoid further changes to data. From this point on, Insta Certifier is the operational CA system and the old RSA Keon system can be shut down.

The RSA Keon migration tools have been tested with Insta Certifier version 7.4 and later. Please contact Insta DefSec for guidance, tools and professional assistance with your CA migration project to Insta Certifier.

INSTA
DefSec

**Further information:**

security.insta.fi
security@insta.fi

Insta DefSec Oy
Sarankulmankatu 20
P.O. Box 80
FI-33901 Tampere, Finland
+358 20 771 7111
www.instadefsec.fi