Entrust Certificate Authority

nShield® HSM Integration Guide for Windows Server

2024-11-20

Table of Contents

Chapter 1. Introduction

The Entrust Certificate Authority is a Public-Key Infrastructure (PKI) solution. The Entrust nShield Hardware Security Module (HSM) securely store and manage encryption keys. This document describes how to integrate both for added security of your PKI.

The HSM is available as an appliance or nShield as a service (nSaaS).

1.1. Product configuration

The integration between the HSM and Certificate Authority has been successfully tested in the following configurations:

Product	Version
Entrust Certificate Authority	v10.2.0
Operating System	Windows Server 2022
PostgreSQL Database	15.2.0

1.2. Supported nShield hardware and software versions

Entrust successfully tested with several nShield hardware and software versions.

Module-protected keys are not supported in Entrust Security Manager v10.0 and later versions. OCS and softcard-protection was tested in all configurations.

1.2.1. nShield

Product	Security World Software	Firmware	Netimage
nSaaS	13.3.2	12.72.1 (FIPS 140-2 certified)	12.80.5

Product	Security World Software	Firmware	Netimage
Connect XC	13.3.2 a	12.50.11 (FIPS 140-2 certified) 12.72.1 (FIPS 140-2 certified) 13.3.1	12.80.4, 12.80.5, 13.4.3
Solo XC	13.3.2	12.72.0 (FIPS 140-2 certified)	
nShield 5c	13.3.2	13.2.2	13.3.2
nShield Edge	13.3.2	12.50.8 (FIPS 140-2 certified)	

1.3. Requirements

To integrate the HSM and Certificate Authority, you have to install the following software packages:

- Security World Software
- a directory service installed and running according to the *Entrust Certificate Authority Directory Configuration Guide*
- PostgreSQL Server
- Certificate Authority 10

Familiarize yourself with:

- the Entrust Certificate Authority (https://www.entrust.com/digital-security)
- the *Installation Guide* and *User Guide* for the HSM
- your organizational certificate policy and certificate practice statement, and a security policy or procedure in place covering administration of the PKI and HSM:
  - the number and quorum of administrator cards in the administrator card set (ACS), and the policy for managing these cards
  - the number and quorum of operator cards in the operator card set (OCS), and the policy for managing these cards
  - the keys protection method: module, softcard, or OCS

- the level of compliance for the Security World, FIPS 140 Level 3
- key attributes such as key size, time-out, or need for auditing key usage

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Install and configure directory service

2.1. Install directory service

The Entrust Certificate Authority requires an LDAP (Lightweight Directory Access Protocol) compliant directory service or a third-party LDAP-compliant X.500 directory. A remote OpenLDAP directory service with a self-signed certificate was used in this integration. See PSIC-Entrust Certificate Authority x for the list of directory services supported.

1. Install the required directory service.
2. Add the following firewall rule if accessing a directory in another server:

```
firewall-cmd --add-port=389/tcp
```

2.2. Configure directory service

The Entrust Certificate Authority directory schema configuration is described in Entrust Certificate Authority 10.2 Documentation Suite - Issue x.

1. Implement the configuration corresponding to your directory service.

   The following directory service parameters are used in this integration:

   - Top Level DN: `dc=entrustsm,dc=local`
   - CA Directory Location: `ou=CAentry,dc=entrustsm,dc=local`
   - Director Administrator: `cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local`
   - First Officer: `cn=FirstOfficer,ou=CAentry,dc=entrustsm,dc=local`

2. Test access to the directory services:

```
C:\Users\Administrator>C:\OpenLDAP\ClientTools\ldapsearch -x -h
ldap://<directory_services_server_IP_or_Name> "cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -b
"cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -s sub -W
Enter LDAP Password: *********
# extended LDIF
#
# LDAPv3
# base <cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# EntrustAdmin, CAentry, entrustsm.local
```

```
dn: cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: entrustadmin
sn: Administrator
userPassword:: e1NTSEF9Vjd2ajd6NFlCWE4yblVLZUc1NjVMbU93VzRMOXd0RzM=
description: Certificate Authority Directory Administratorr
cn: EntrustAdmin

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Chapter 3. Install and configure the Entrust nShield HSM

3.1. Select the protection method

OCS, Softcard, or Module protection can be used to authorize access to the keys protected by the HSM. Follow your organization's security policy to select an authorization access method.

3.2. Install the HSM

Install the nShield Connect HSM locally, remotely, or remotely via the serial console. See the following nShield Support articles and the *Installation Guide* for the HSM:

- How to locally set up a new or replacement nShield Connect
- How to remotely set up a new or replacement nShield Connect
- How to remotely set up a new or replacement nShield Connect XC Serial Console model

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

3.3. Install the nShield Security World Software and create the Security World

To install the nShield Security World Software and create the Security World:

1. Install the Security World software as described in *Installation Guide* and the *User Guide* for the HSM. This is supplied on the installation disc.
2. Add the Security World utilities path `C:\Program Files\nCipher\nfast\bin` to the system path.
3. Open the firewall port 9004 for the HSM connections.
4. Open a command window and run the following to confirm the HSM is `operational`.

```
# enquiry
Server:
```

```
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        530E-02E0-D947 7724-8509-81E3 09AF-0BE9-53AA 9E10-03E0-D947
 mode                 operational
...
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        530E-02E0-D947
 mode                 operational
 ...
```

5. Create your Security World if one does not already exist, or copy an existing one. Follow your organization's security policy for this. Create extra ACS cards as spares in case of a card failure or a lost card.

ACS cards cannot be duplicated after the Security World is created.

6. Confirm the Security World is `usable`.

```
# nfkminfo
World
 generation  2
 state       0x37270008 Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
 ...
```

3.4. Generate the OCS or Softcard in the CA server

The OCS or Softcard and associated passphrase will be used to authorize access to the keys protected by the HSM. Typically, one or the other will be used, but rarely both.

When selecting your protection method take into consideration:

1. Your organization's security policy.
2. Unattended startup requirements.

The OCS or Softcard needs to the presented initially when configuring the Entrust Certificate Authority Manager. In production, unattended startup is possible in some scenarios.

3.4.1. Create the OCS

To create the OCS:

1. Ensure file `C:\ProgramData\nCipher\Key Management Data\config\cardlist` contains the serial number of the card(s) to be presented, or the wildcard "*".
2. Open a command window as an administrator.
3. Run the `createocs` command as described below, entering a passphrase or password at the prompt.

   Create one card for each person with access privilege, plus the spares.

   The **--persist** option allows for removal of the OCS for save storage. Otherwise, the authentication provided by the OCS is only available while the OCS card is inserted in the HSM front panel slot, or the TVD. Note that `slot 2`, remote via a Trusted Verification Device (TVD), is used to present the card.

   After an Operator Card Set has been created, the cards cannot be duplicated.

```
# createocs -m1 -s2 -N testOCS -Q 1/1 --persist

FIPS 140-2 level 3 auth obtained.

Creating Cardset:
 Module 1: 0 cards of 1 written
 Module 1 slot 0: Admin Card #1
 Module 1 slot 2: empty
 Module 1 slot 3: empty
 Module 1 slot 2: blank cardSteps:

 Module 1 slot 2:- passphrase specified - writing card
Card writing complete.

cardset created; hkltu = a165a26f929841fe9ff2acdf4bb6141c1f1a2eed
```

4. Verify the OCS was created:

```
# nfkminfo -c
Cardset list - 1 cardsets:  (P)ersistent/(N)ot, (R)emoteable/(L)ocal-only
 Operator logical token hash              k/n timeout  name
 02466cfb08d1115802ebe39920bc562b43b0d43b  1/1  none-PL testOCS
```

   The `rocs` utility also shows the OCS was created:

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardset
No. Name                    Keys (recov) Sharing
  1 testOCS                 2 (2)        1 of 1; persistent
rocs> quit
```

3.4.2. Create a Softcard

To create a Softcard:

1. Run the following command, and enter a passphrase or password at the prompt:

```
# ppmk -n EntrustSNSoftcard

Enter new pass phrase:
Enter new pass phrase again:
New softcard created: HKLTU d9414ed688c6405aab675471d3722f8c70f5d864
```

2. Verify the Softcard was created:

```
# nfkminfo -s
SoftCard summary - 1 softcards:
 Operator logical token hash               name
 d9414ed688c6405aab675471d3722f8c70f5d864  testSC
```

   The `rocs` utility also shows that the OCS and Softcard were created:

```
# rocs
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cards
No. Name                    Keys (recov) Sharing
  1 testOCS                 2 (2)        1 of 1; persistent
  2 testSC                  0 (0)        (softcard)
rocs> quit
```

Chapter 4. Install the Entrust Certificate Authority

4.1. Install the Entrust Certificate Authority PostgreSQL

Certificate Authority requires a database to store information about the Certification Authority, X.509 users, and EAC entities. For a list of supported databases, see *PSIC-Entrust Authority Security Manager 10.0*.

In this guide, an embedded Certificate Authority PostgreSQL database is used. This database will be installed on the same server that will host Certificate Authority.

For information more about installing and configuring Certificate Authority PostgreSQL Database, see the *Security Manager Database Configuration Guide*.

If you are using your own supplied database, Entrust strongly recommends that you install the database on its own dedicated server. To install and configure (or upgrade) your chosen database, read your database documentation and the *Security Manager Database Configuration Guide*.

To install and use Certificate Authority in a cluster, you must use your own supplied database. The Entrust-supplied Certificate Authority PostgreSQL Database does not support a clustered environment.

To install PostgreSQL Server on the server machine:

1. Download the PostgreSQL Server installer for the Windows operating system (`EntrustCertificateAuthorityPostgreSQL.15.2.0.22.msi`) from the Entrust TrustedCare online support site.
2. To start installing the PostgreSQL database for Certificate Authority, double-click the setup file `EntrustCertificateAuthorityPostgreSQL.15.2.0.22.msi`.

   An installation wizard appears.

3. Select **Next**.
4. In the **PostgreSQL Database Folders** window, accept the default, then select **Next**.
5. In the **PostgreSQL Windows Account Password** window, set the password for **easm_entrust_pg** account, then select **Next**.

6. In the **PostgreSQL Databases Accounts** window, provide the password for the **easm_entrust** and **easm_entbackup** accounts and select **Next**.
7. In the **PostgreSQL Database Port** window, accept the default, select **Next**.
8. In the **Check Setup Information** window, review and select **Next**.
9. In the **Ready to Install** window, select **Install**.
10. In the **Install Wizard Complete** dialog, select **Finish**.
11. Close any open windows or dialogs.
12. If you do not see the setup dialogs when installing PostgreSQL, run the `ent_setup.bat` file found at: `C:\Program Files\Entrust\easm_postgres15\dbserver\bin`. Follow the same instructions as above but in CLI format.

For example:

```
[ent_setup] Logging to 'C:\Users\Administrator\AppData\Roaming\Entrust\postgresql\ent_setup.log'.
[ent_setup]
[ent_setup] ********************************************************
[ent_setup] Starting setup...
[ent_setup] ********************************************************
[ent_setup] Welcome to the Entrust Certificate Authority PostgreSQL Database 15.2 setup.
[ent_setup]
[ent_setup] Checking for a previous version...
[ent_setup]    Registry key [HKLM:\SOFTWARE\Entrust\PostgreSQL\11] does not exist, no installation found.
[ent_setup]
[ent_setup] Checking for current version...
[ent_setup]    Found InstallDir [C:\Program Files\Entrust\easm_postgres15\].
[init]
[init] No upgradeable Entrust Authority Security Manager PostgreSQL Database installation was found.
[init]
[init] Do you wish to initialize Entrust Certificate Authority PostgreSQL Database 15.2 at this time? (y/n): y
[init] Performing a full initialization for installation at [C:\Program Files\Entrust\easm_postgres15]...
[init]
[init] Checking for 'easm_entrust_pg' OS user...
[init]    User was not found, creating OS user 'easm_entrust_pg'...
[init]
[init]    ***NOTE***: Be sure to adhere to any of your organization's password rules as well.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entrust_pg': ***********
[init] Please confirm the password for: 'easm_entrust_pg': ***********
[init]    The 'easm_entrust_pg' user has been successfully created.
[init]    Enabling SeServiceLogonRight for easm_entrust_pg...
[init]
[init] Please choose a listen port for the server [5432]:
[init]
[init] Please choose a location for the PostgreSQL Data directory : [c:\eca_pg_data\15]:
[init] Adding full (inheritable) permission for [easm_entrust_pg] to location [c:\eca_pg_data\15]...
[init] Adding full (inheritable) permission for [Administrators] to location [c:\eca_pg_data\15]...
[init] Adding full (inheritable) permission for [ENTRUST-SM-WIND\Administrator] to location [c:\eca_pg_data
\15]...
[init]
[init] Please choose a location for the PostgreSQL Wal directory : [c:\eca_pg_wal\15]:
[init] Adding full (inheritable) permission for [easm_entrust_pg] to location [c:\eca_pg_wal\15]...
[init] Adding full (inheritable) permission for [Administrators] to location [c:\eca_pg_wal\15]...
[init] Adding full (inheritable) permission for [ENTRUST-SM-WIND\Administrator] to location [c:\eca_pg_wal\15]...
[init]
```

```
[init] Initializing Database cluster with database super user 'easm_entrust_pg'...
[init]
[init] Calculating the recommended shared_buffers value...
[init] Installing and updating custom pg_easm_DB.conf...
[init]    Setting archive_command path to C:\Program Files\Entrust\easm_postgres15\bin\pg_archwal.bat
[init]    Setting port = 5432
[init]    Setting shared_buffers = 2048
[init] Updating postgresql.conf...
[init]    Setting include = pg_easm_DB.conf
[init]    The database cluster is initialized.
[init] Setting EASMPOSTGRESDIR environment variable...
[init] Setting OPENSSL_CONF environment variable...
[init]
[init] Registering PostgreSQL Server as a Windows service...
[init]
[init] Setting PostgreSQL service display name and description...
[init]
[init] Starting the PostgreSQL service...
[init]
[init] Creating database easm_DB...
[init]
[init] A database user 'easm_entrust' is required.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entrust': ***********
[init] Please confirm the password for: 'easm_entrust': ***********
[init] Creating 'easm_entrust' user...
[init]
[init] A database backup role 'easm_entbackup' is required.
[init]
[init] The following characters cannot be used when choosing the password:
[init]    < > # \ " / | ' ^ ; &  <space> <tab>
[init] Please choose a password for:    'easm_entbackup': ***********
[init] Please confirm the password for: 'easm_entbackup': ***********
[init] Creating 'easm_entbackup' database role...
[init]
[init] Creating easm_entrust schema...
[init] Creating extension pgrowlocks...
[init] Creating extension pg_freespacemap...
[init] Creating extension pgstattuple...
[init] Creating extension pg_buffercache...
[init] Creating extension pageinspect...
[init]
[init] Removing full (inheritable) permission for [ENTRUST-SM-WIND\Administrator] from location [c:\eca_pg_data
\15]...
[init] Removing full (inheritable) permission for [ENTRUST-SM-WIND\Administrator] from location [c:\eca_pg_wal
\15]...
[init]
[init] Registering PostgreSQL event DLL for [C:\Program Files\Entrust\easm_postgres15]...
[init]
[init] Setting PGPORT environment variable...
[init]
[init] Stopping the PostgreSQL service...
[init]
[init] Starting the PostgreSQL service...
[ent_setup]
[ent_setup] Operation complete!
```

Make a note of these users and passwords as this information will be needed later in the setup.

4.2. Install the Entrust Certificate Authority

To install Entrust Certificate Authority on the server computer:

1. Download the Certificate Authority for Windows (`EntrustCertificateAuthority.10.2.0.119.msi`) from the Entrust TrustedCare online support site.
2. Run the installation program.

   The install wizard will launch and install the software.

   The installation path after the install will be `C:\Program Files\Entrust`.

3. Once the installation completes, select **Finish** in the **Install Wizard Complete** dialog.
4. Preload the OCS or Softcard as described in Establish a preload session if you have not done this yet.
5. Install OpenLDAP for Windows on the client if you have not yet done so.
6. Test access to the directory service from the Certificate Authority server:

```
C:\Users\Administrator>C:\OpenLDAP\ClientTools\ldapsearch -x -h <directory_services_server_IP_or_Name>
"cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -b "cn=EntrustAdmin,ou=CAentry,dc=entrustsm,dc=local" -s
sub -W
```

Chapter 5. Configure the Entrust Certificate Authority

5.1. Establish a preload session

You can use an OCS or Softcard to establish connection with the HSM. Before installing Certificate Authority, you must preload the OCS or Softcard that is used to protect the Entrust keys. If you are using a K-of-N OCS, this section assumes the OCS has been created. Refer to your *Security World User Guide* on how to create an OCS or Softcard. You must decide which method you will use for the connection before proceeding.

To initialize Certificate Authority, the OCS or Softcard has to be preloaded.

1. Edit the `cknfastrc` environment variables. The `cknfastrc` file can be found in `%NFAST_HOME%\cknfastrc`. Edit the file to include:

```
# Softcard
CKNFAST_LOADSHARING=1

# Enable Module Protection
CKNFAST_FAKE_ACCELERATOR_LOGIN=1

# Other variables
CKNFAST_NO_UNWRAP=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none

# Preload file location
NFAST_NFKM_TOKENSFILE=C:\preload\<filename>

# PCKS #11 log level and file location
CKNFAST_DEBUG=10
CKNFAST_DEBUGFILE=C:\preload\pkcs11.log
```

   Useful information about environment variables:

   - The filename in this line: 'NFAST_NFKM_TOKENSFILE=C:\preload\<filename>' is user defined and will be referenced in the `preload` command. For example, `%NFAST_HOME%\Bin>preload -c <OCS Name> -f <pathname to preload file and filename> pause`.
   - When using a K-of-N Card Set where K>1, set `CKNFAST_LOADSHARING=0`. When using a K-of-N Card Set where K=1, set `CKNFAST_LOADSHARING=1`. This also applies to when using Softcards.
   - For Enhanced Database Protection (EDP) use `CKNFAST_LOADSHARING=0` after enabling the database hardware protection. Restart the system for load

sharing to work.

- When you are using nShield with ePassport CVCA, use `CKNFAST_ASSUME_SINGLE_PROCESS=0`. If ePassport Document Verifier Certificate requests are canceled, this setting ensures that the associated physical key is deleted in the HSM. For information on environment variables, see the *User Guide* for the HSM.

For more information about the environment variables used in `cknfastrc`, see the *nShield PKCS11 library environment variables* section in the *User Guide* for the HSM.

2. Create an empty folder called `Preload` on drive `C:`.
3. Right-click on a command prompt and select **Run as Administrator** and navigate to `%NFAST_HOME%\bin>`.
4. Run the following command to list the OCS:
   - For K-of-N OCS:

     ```
     % nfkminfo.exe -c
     ```

   - For Softcard:

     ```
     % nfkminfo.exe -s
     ```

5. Open a command window to run preload exclusively.

   Do not close this window throughout the Entrust Certificate Authority configuration. Otherwise the configuration will fail.

6. Preload the Card Set by running the `preload -c` command for OCS, or `preload -s` command for Softcard.

   ```
   # preload -<c/s> <OCS/Softcard> -f <location of user defined file in cknfastrc> pause
   ```

   Present the OCS cards and passphrase when prompted.

   For example:

   ```
   % preload -c testOCS -f C:\preload\entrustsmtoken pause
   2024-10-09 19:10:02: [6352]: INFO: Preload running with: -c testOCS -f C:\preload\entrustsmtoken pause
   2024-10-09 19:10:02: [6352]: INFO: Created a (new) connection to Hardserver
   2024-10-09 19:10:02: [6352]: INFO: Modules newly usable: [1].
   2024-10-09 19:10:02: [6352]: INFO: Found a change in the system: an update pass is needed.
   2024-10-09 19:10:02: [6352]: INFO: Loading cardset: testOCS in modules: [1]
   ```

```
Loading `testOCS':
 Module 1 slot 3: `testOCS' #2
 Module 1 slot 0: empty
 Module 1 slot 2: empty
 Module 1 slot 4: empty
 Module 1 slot 5: empty
 Module 1 slot 3:- passphrase supplied - reading card
Card reading complete.

2024-10-09 19:10:15: [6352]: INFO: Stored Admin key: kfips (003e...) in module #1
2024-10-09 19:10:15: [6352]: INFO: Loading cardset: Cardset: testOCS (edb3...) in module: 1
2024-10-09 19:10:15: [6352]: INFO: Stored Cardset: testOCS (edb3...) in module #1
2024-10-09 19:10:15: [6352]: INFO: Maintaining the cardset testOCS protected
key(s)=['pkcs11:ucedb3d45a28e5a6b22b033684ce589d9e198272c2-f40e2f7b44bdcbf04d449e254de978d017a81b2c'].
2024-10-09 19:10:15: [6352]: INFO: The private/symmetric key
pkcs11/ucedb3d45a28e5a6b22b033684ce589d9e198272c2-f40e2f7b44bdcbf04d449e254de978d017a81b2c is loaded in
module(s): [1].
2024-10-09 19:10:15: [6352]: INFO: Loading complete. Now pausing...
```

If non-persistent cards are used, then the last card in the quorum must remain inserted in the card reader. If persistent cards are used, then the last card in the quorum can be removed from the card reader.

The filename is user defined but must be consistent when setting the variable in `cknfastrc` and invoking `preload`. For example: **A variable set in `cknfastrc`:** `NFAST_NFKM_TOKENSFILE=C:\Preload\filename` A variable invoked with `preload`: `>preload.exe -c ocsname -f "C:\Preload\filename" pause` ** Both should use the path to the same user defined file, initially defined in 'cknfastrc'

7. Confirm the OCS or Softcard has been preloaded by opening a separate command window and running the following command. You must keep the `preload` command window active. You can minimize it but do not close it, otherwise you will shut down the session. The loaded **Objects** will be reported.
   - For K-of-N OCS:

     ```
     % preload.exe -c <cardsetname> -f <pathname>\<filename> nfkminfo
     ```

   - For Softcard:

     ```
     % preload -s <softcardname> -f <pathname>\<filename> nfkminfo
     ```

   For example:

   ```
   % preload.exe -c testOCS -f
   ```

```
...

C:\preload\entrustsmtoken nfkminfo
Pre-Loaded Objects (  3):  objecthash   module objectid  generation
 003e04e3c07fb5791f651c992da5527779159f87   1 0x5b2a083c 1
 edb3d45a28e5a6b22b033684ce589d9e198272c2   1 0x5b2a0839 1
 744bff70468d7ec74162d859447a4b15c3554ed6   1 0x5b2a083a 1
```

Useful information concerning Operator Card Sets (OCS):

- You must present sufficient different OCS cards to fulfill the quorum. The passphrase (if any) can be different for each OCS card.
- If non-persistent cards are used, then the last card in the quorum must remain inserted in the card reader.
- If persistent cards are used, then the last card in the quorum can be removed from the card reader.
- The tokens file is generated by the `preload` utility and is valid for one continuous session only. If the session is lost, then the token authorization is lost. You cannot reuse the same token file once the session is lost, even if you will use the exact same OCS cards again. To restart, you must delete the expired tokens file, and will have to go through the entire preload sequence again.
- A session, and tokens authorization may be lost if:
  - There is a temporary power failure
  - You remove the last card in the quorum if they are non-persistent OCS cards
  - You clear the module.

The tokens file represents a security risk if permissions to access it are not restricted to authorized persons only.

5.2. nShield Edge pre-configuration

If you are using an nShield Edge device, it is necessary to adjust the `.ini` file settings for Certificate Authority in order to allow for a sufficient timeout duration for the system to initialize properly. The nShield Edge exhibits slower service startup times with respect to operations, which is to be expected. Therefore, in order to ensure optimal performance, it is recommended that the timeout settings be configured appropriately in the `.ini` file.

Navigate to the `ini` directory:

- By default: `C:\Program Files\Entrust\Certificate Authority\etc\ini\entMgr.ini`
- Edit the `entMgr.ini` file in the **[login]** section and add this setting:

```
serviceStartStopWaitSeconds=3600
clusterStartWaitSeconds=1800
clusterStopWaitSeconds=300
```

5.3. Configure the Entrust Certificate Authority

This section describes how to configure Entrust Certificate Authority. You can configure Certificate Authority immediately after you install it. You must configure Certificate Authority before you can initialize it. (Initializing Certificate Authority allows you to use Certificate Authority).

When you configure Certificate Authority:

- You provide data that allows Certificate Authority to connect to your directory and the Certificate Authority database.
- You then choose certificate algorithms, lifetimes, and other options for your Certification Authority.

You can only configure Certificate Authority once. If you make a mistake configuring Certificate Authority, you can change some of the settings by editing the `entmgr.ini` file, or you can uninstall Certificate Authority, then reinstall and configure it.

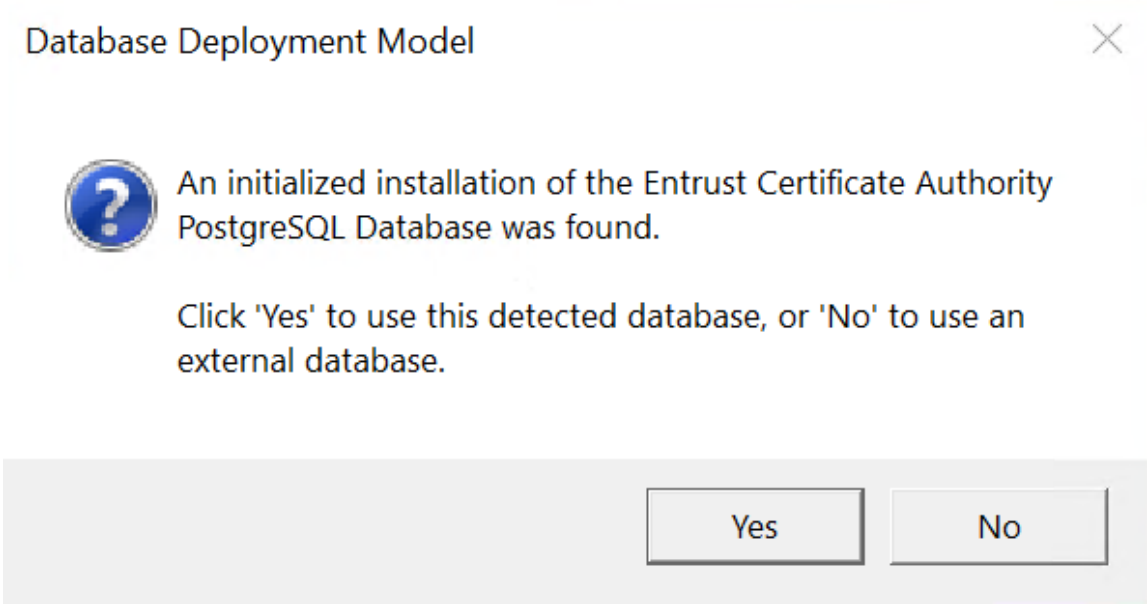
To configure Certificate Authority:

1. Navigate to the Certificate Authority `\bin` directory.

   By default, this is: `C:\Program Files\Entrust\Certificate Authority\bin`.

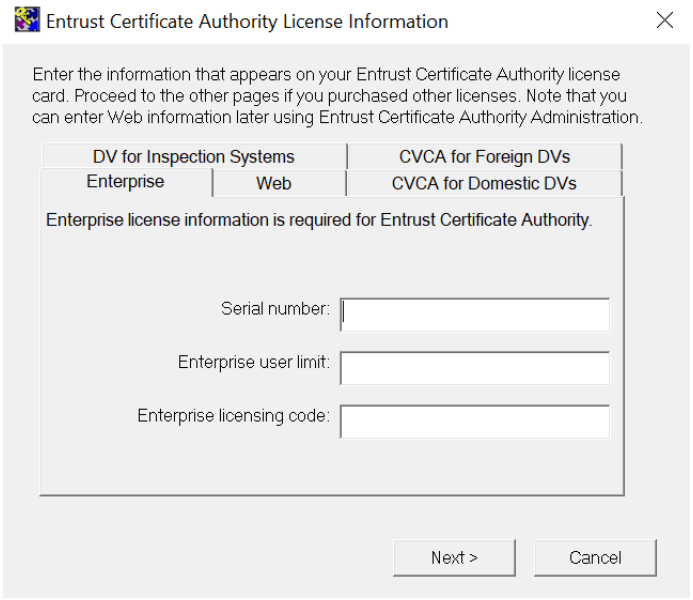
2. Double-click `entConfig.exe`.

   The **Database Deployment Model** dialog appears.



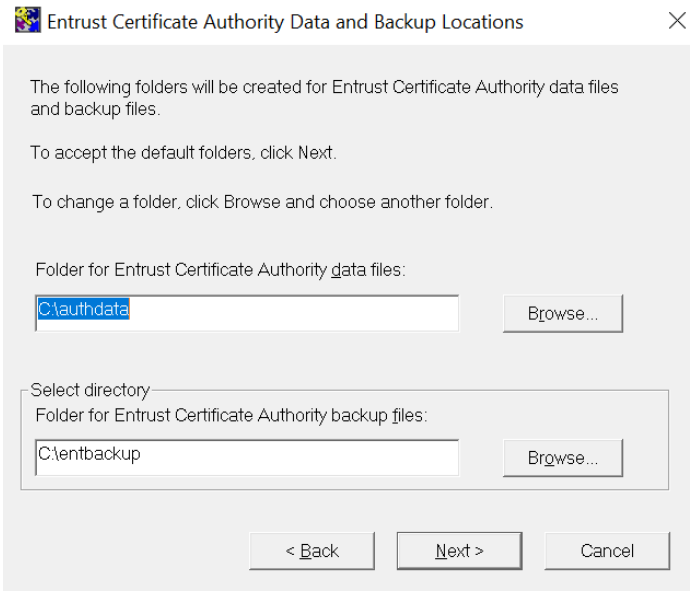
3. Select **Yes**.
4. In the **Entrust Certificate Authority Configuration** dialog, select **Next**.

   The **Certificate Authority License Information** dialog appears.



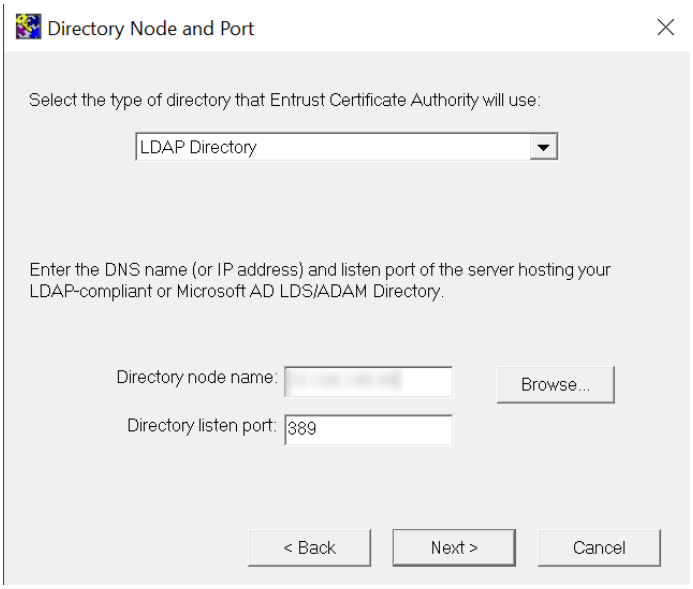
5. Enter the Enterprise licensing information that appears on your Entrust licensing card:
   - **Serial Number**
   - **Enterprise user limit**
   - **Enterprise licensing code**
6. Select **Next**.

   The **Certificate Authority Data and Backup Locations** dialog appears.



7. Accept the defaults:
   - For the data files, the default is `c:\authdata`.
   - For the backup files, the default is `c:\entbackup`.
8. Select **Next**.

   The **Directory Node and Port** dialog appears.

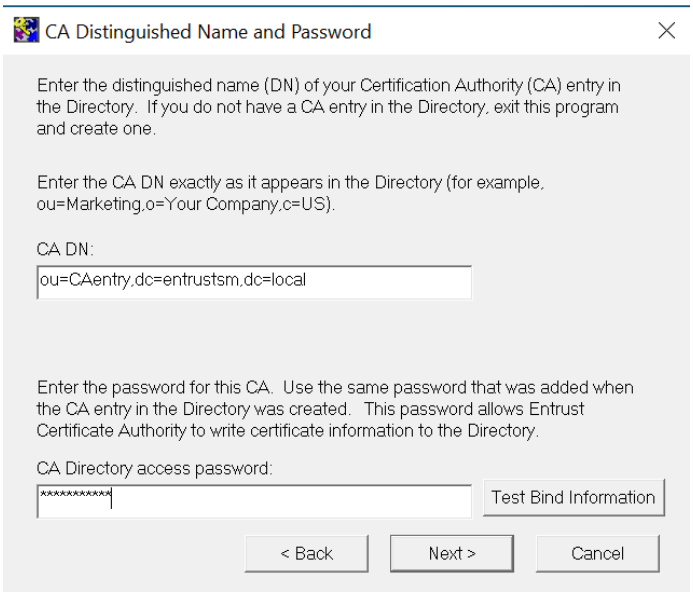


9. Enter the required details:
   - Select the type of directory that the Certificate Authority will use, for example: **LDAP Directory**.
   - Enter the **Directory node name** (server name or IP address) of your directory services server.

- Set the **Directory listen port** to 389.

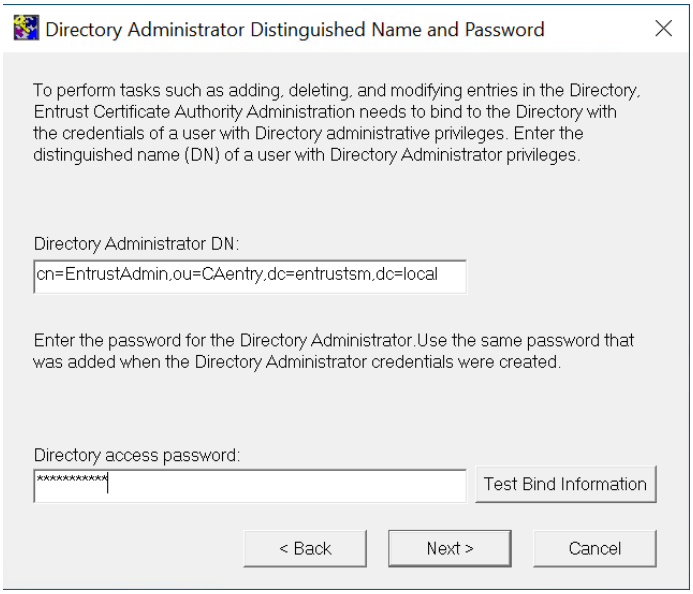
10. Select **Next**.

    The **CA Distinguished Name and Password** dialog appears.



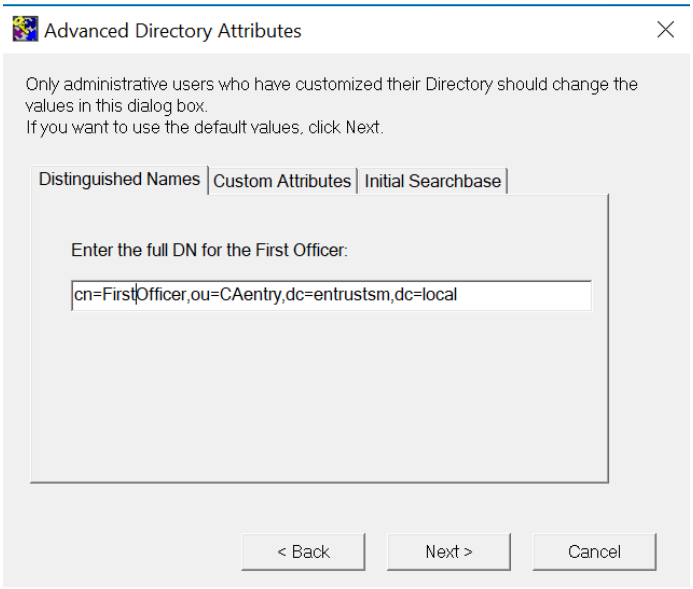
11. Enter the **CA DN** and **CA Directory access password**, which you provided when you were configuring the Directory Services for use with Certificate Authority, see Install the Entrust Certificate Authority.
12. Select **Test Bind Information**.
    - If the bind is successful, select **OK**.
    - If the bind is unsuccessful, ensure that the server name or IP address are correct, and that the Directory Services is running and retest using the following information:
      - Set **CA DN** to `o=CA<name>`.
      - Enter the **CA Directory access password**.
13. Select **Next**.

    The **Directory Administrator Distinguished Name and Password** dialog appears.



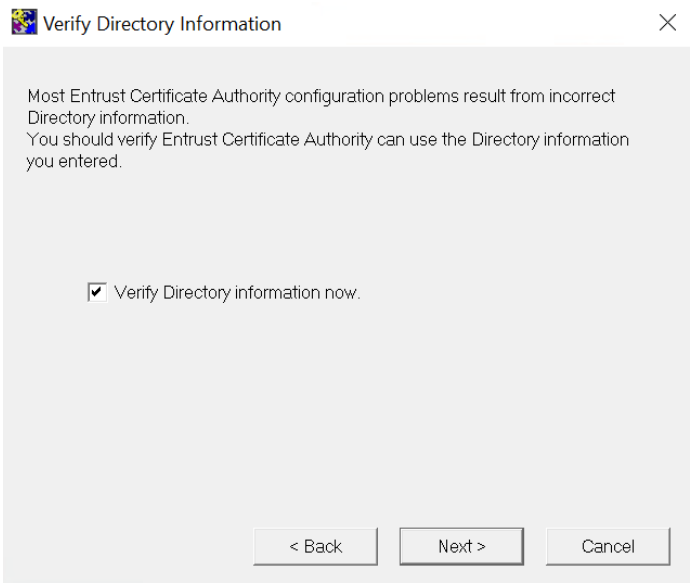
14. Enter the distinguished name and password details:
    - Enter the **Directory administrator DN** as `cn=diradmin,ou=CA,o=Entrust`.
    - Enter the **Directory access password**.
15. Select **Test Bind Information**.
    - If the bind is successful, select **OK**.
    - If the bind is unsuccessful, ensure that the server name or IP address are correct, and that the Directory Services is running and retest using the following information:
        - Set **Directory administrator DN** to `cn=<manager>`.
        - Enter the **Directory access password**.
16. Select **Next**.

    The **Advanced Directory Attributes** dialog appears. This displays the distinguished name for the First Officer.



17. Verify the information for the First Officer is correct. This should follow the `cn=First Officer, o=CA<name>` general format.
18. Select **Next**.

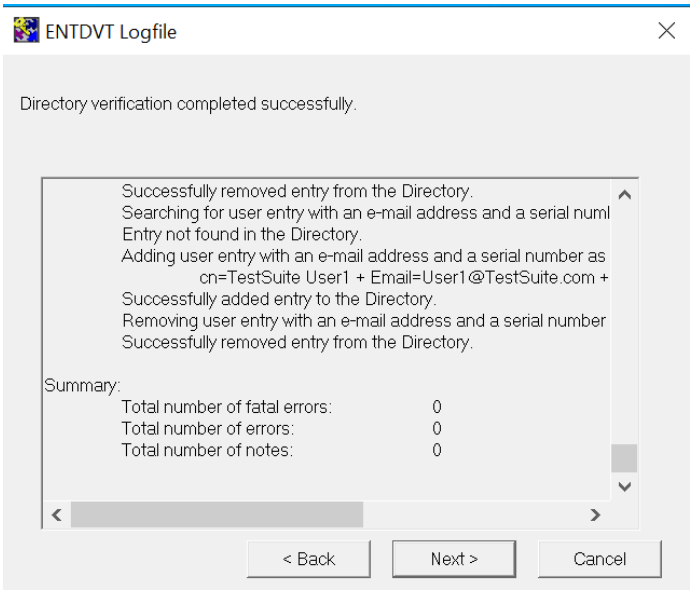
    The **Verify Directory Information** dialog appears.



19. Select **Verify Directory information now**, then select **Next**.

    The **ENTDVT Logfile** page appears.

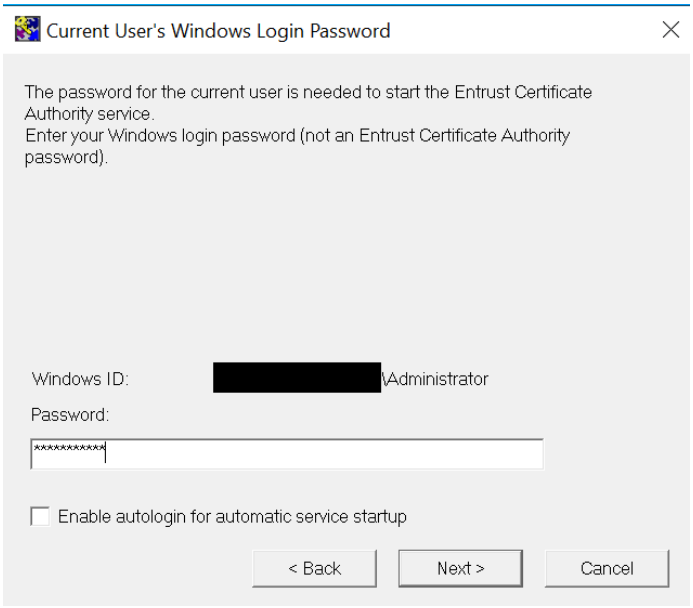
    The Entrust Directory Verification Tool (**EntDVT**) will verify the settings. At the bottom of the dialogue there should be no errors in the **Summary** section. For example:



If there are errors on the results, you need to address them in your directory services setup before proceeding.

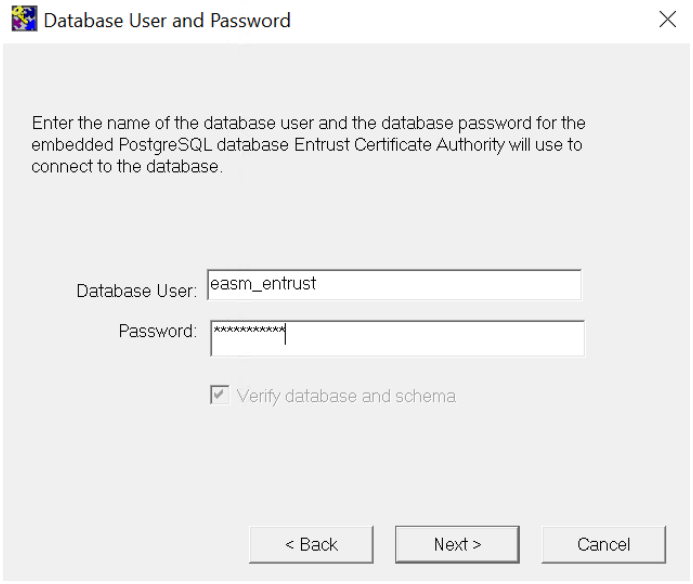
20. Select **Next**.

    The **Current User's Windows Login Password** dialog appears.



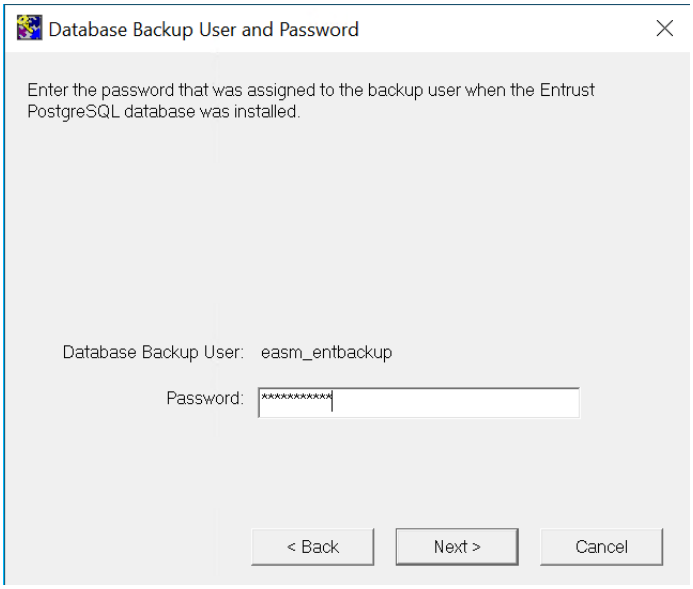
21. Log in with your Windows credentials.
22. Clear the **Enable autologin for automatic service startup** checkbox.
23. Select **Next**.

    The **Database User and Password** dialog appears.



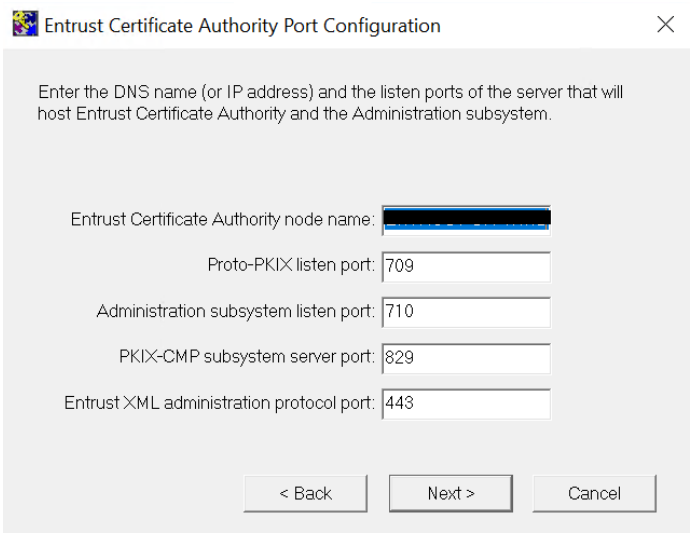
24. Enter the password that was assigned to **easm_entrust** when you installed the PostgreSQL Server, see Install the Entrust Certificate Authority, then select **Next**.

    The **Database User and Password** dialog appears.



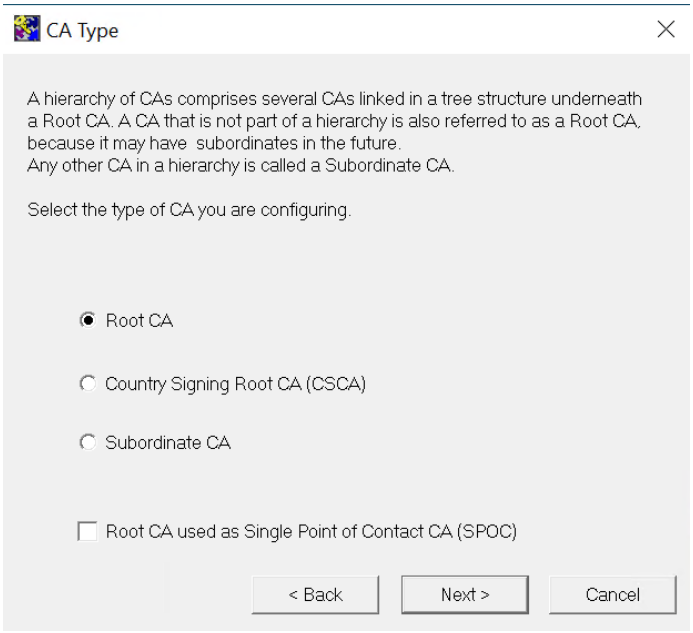
25. Enter the password that was assigned to the **backup** user when you installed the PostgreSQL Server, see Install the Entrust Certificate Authority, then select **Next**.

    The **Certificate Authority Port Configuration** dialog appears.



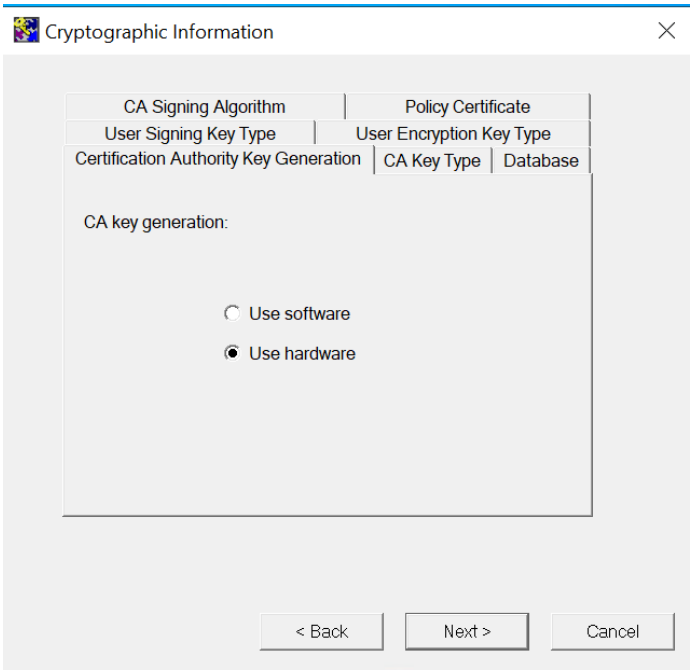
26. Accept the defaults, then select **Next**.

    The **CA Type** dialog appears.

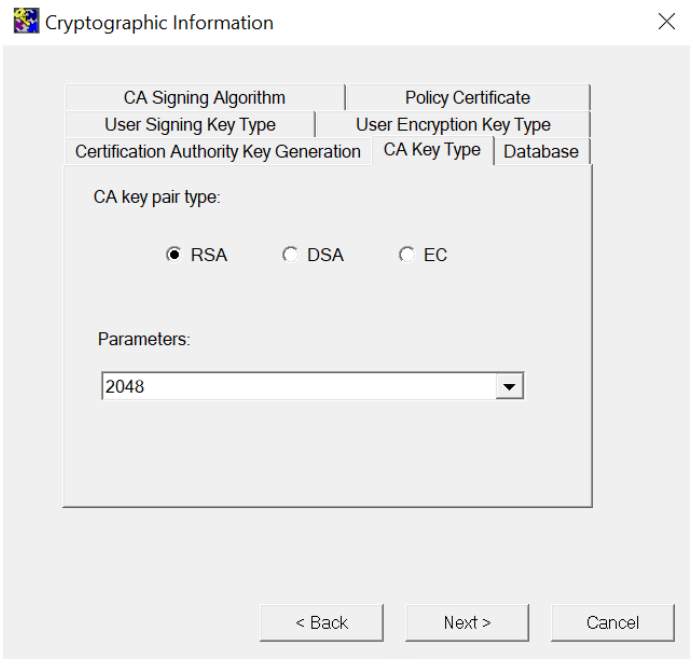


27. Choose the default **Root CA** option, ensure that the **Root CA used as Single Point of Contact CA (SPOC)** box remains unchecked, and then select **Next**.

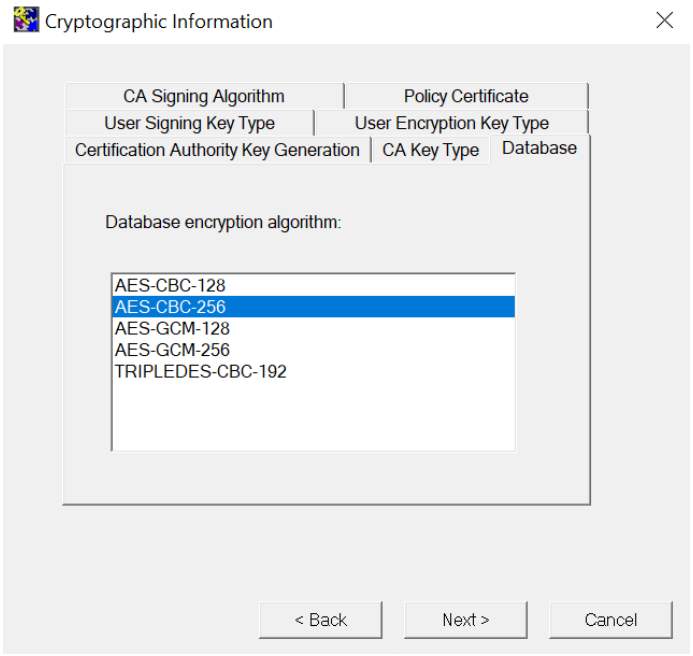
    The **Cryptographic Information** dialog appears.



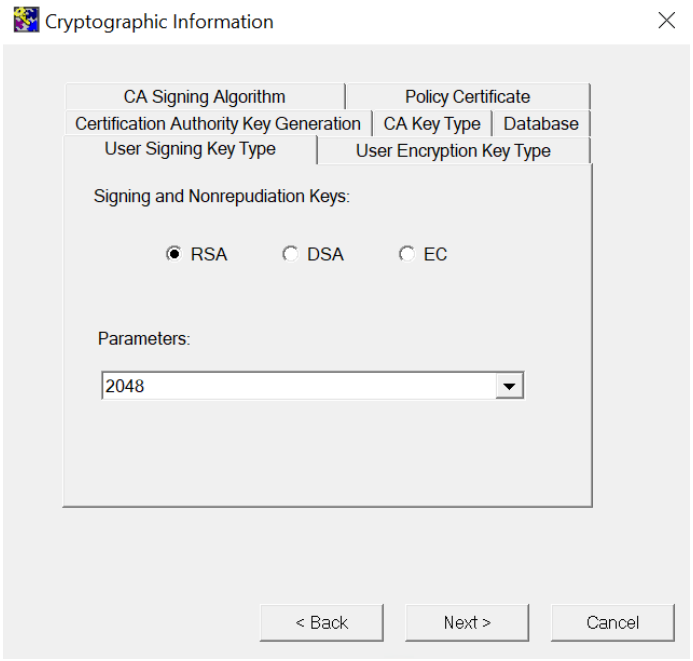
28. Select the **Certification Authority Key Generation** tab, select **Use hardware**, then select **Next**.
29. On the **CA Key Type** tab, which defines the CA key pair type and parameters, accept the defaults, then select **Next**.



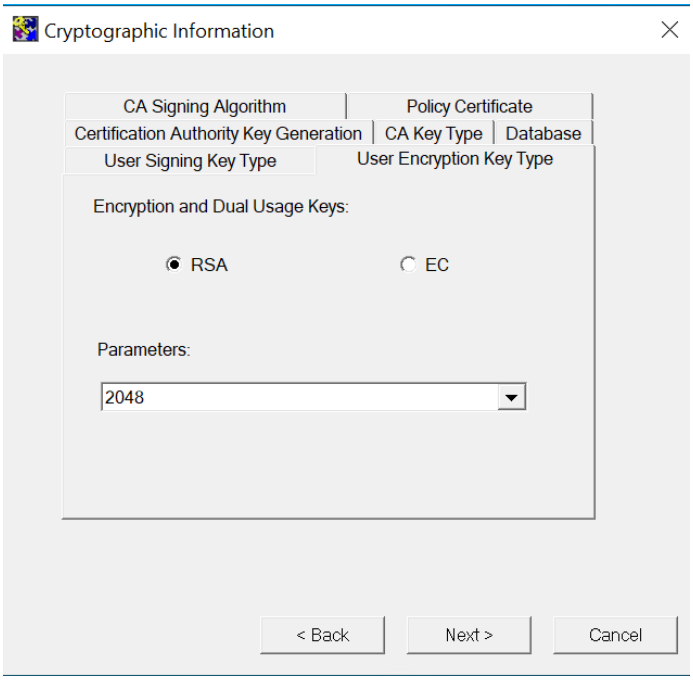
30. On the **Database** tab, which defines the database encryption algorithm, accept the default, then select **Next**.



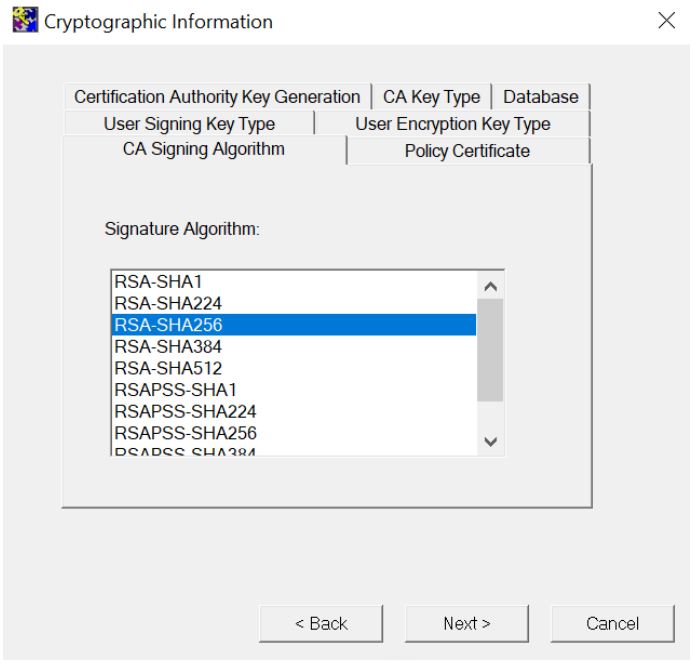
31. On the **User Signing Key Type** tab, which defines the key pair type and parameters for user signing keys, accept the defaults, then select **Next**.



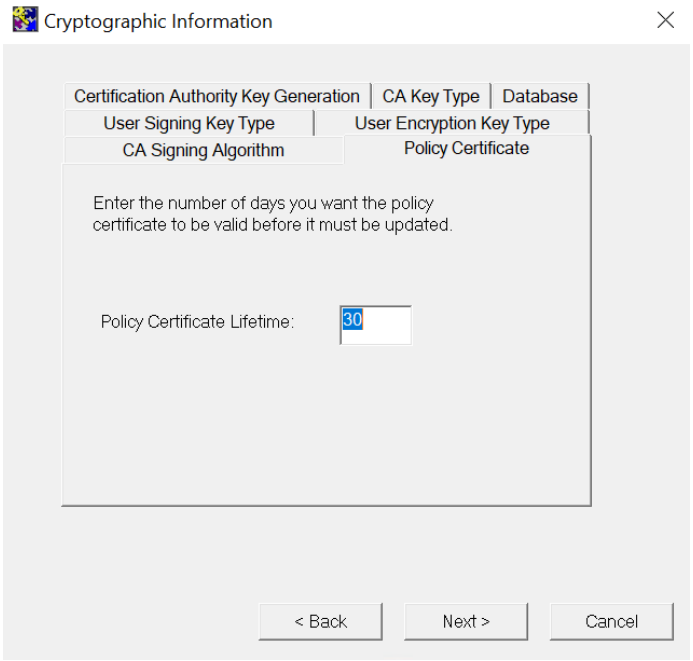
32. On the **User Encryption Key Type** tab, which defines the key pair type and parameters for user encryption keys, accept the defaults, then select **Next**.



33. On the **CA Signing Algorithm Type** tab, accept the default, then select **Next**.

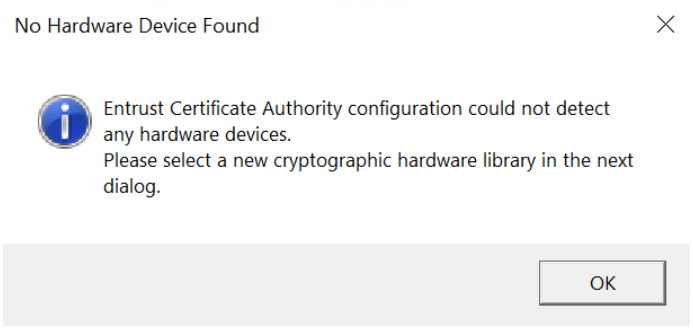


34. On the **Policy Certificate** tab, which defines the lifetime of the Entrust policy certificate, accept the default, then select **Next**.



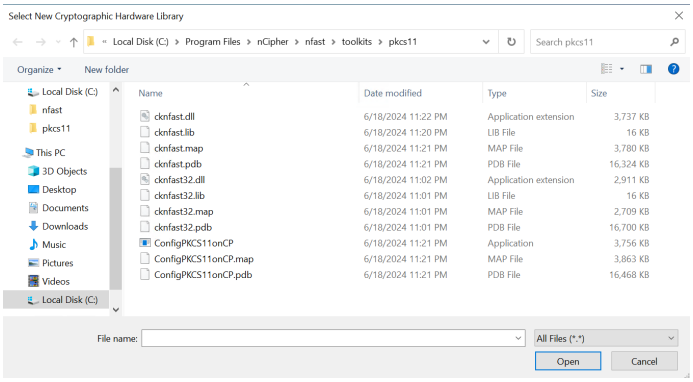
For this integration to work with EC-P and RSAPSS, the ECC activation feature must be enabled for the nShield HSM. In the `%NFAST_ HOME%\bin` directory, run `FET.exe`.

The **No Hardware Device Found** dialog appears.



35. Select **Ok**.

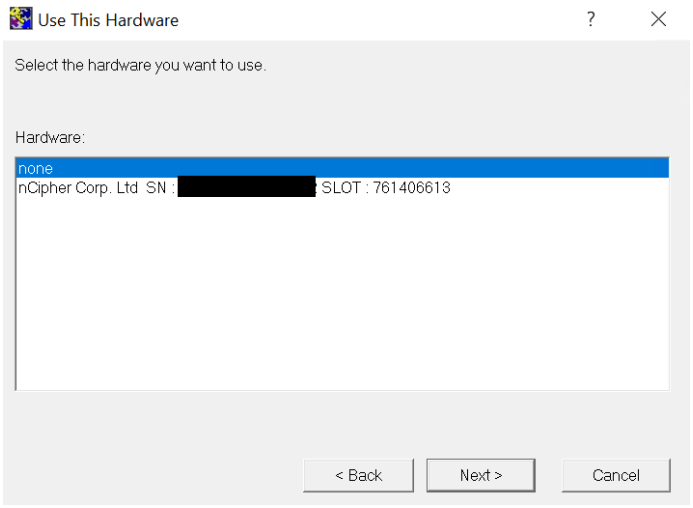
A file explorer opens.



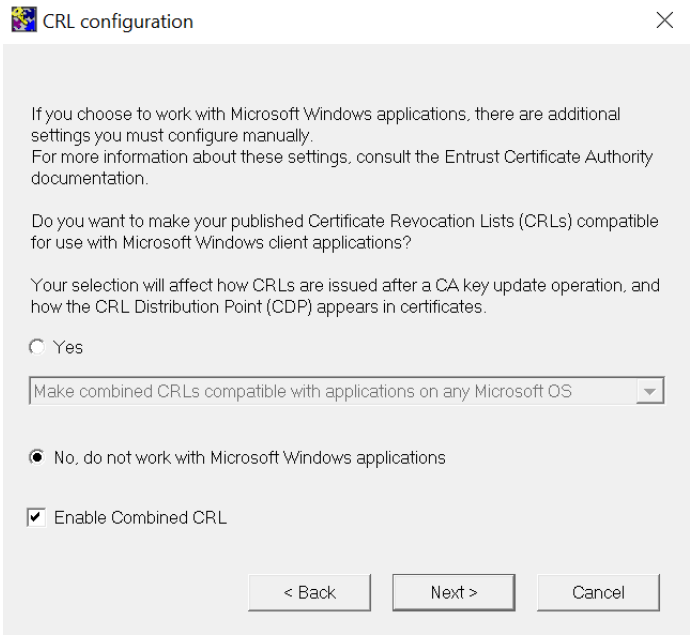
36. To select the nShield PKCS11 library, navigate to and select `%NFAST_HOME%\toolkits\pkcs11\cknfast.dll`.

You can confirm this location by opening the `entmgr.ini` file located in the `Entrust` directory and looking for the `CryptokiV2LibraryNT = C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll` entry.

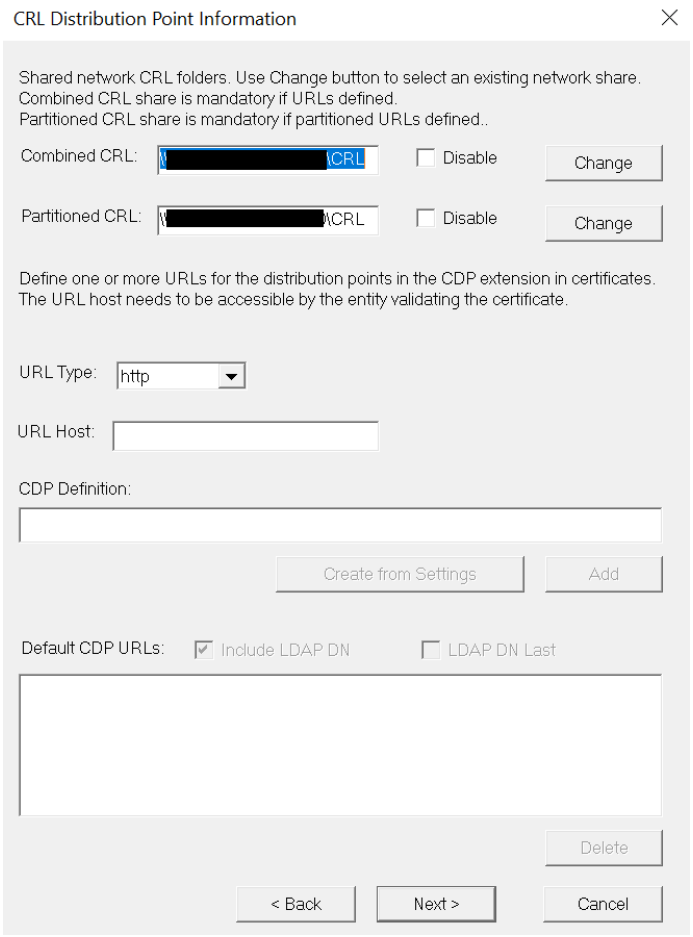
37. In the **Use This Hardware** dialog, select the HSM slot, then select **Next**.



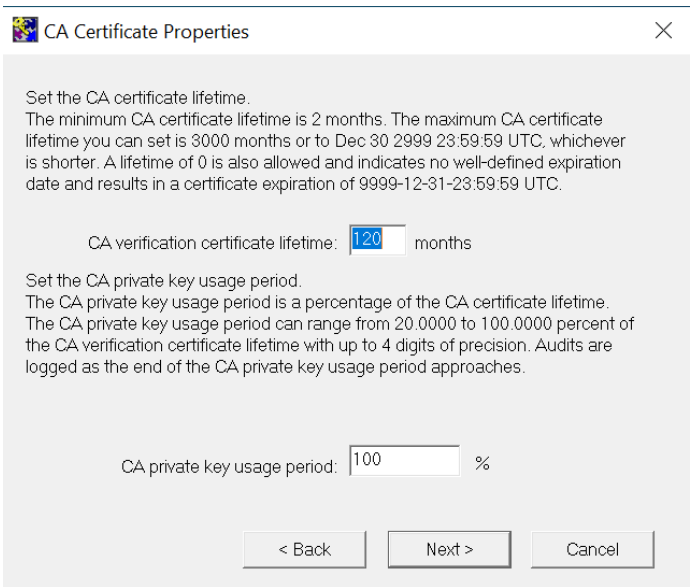
38. In the **CRL Configuration** dialog, select **No, do not work with Microsoft Windows applications**, then select **Next**.



39. In the **CRL Distribution Point** dialog, accept the defaults, then select **Next**.

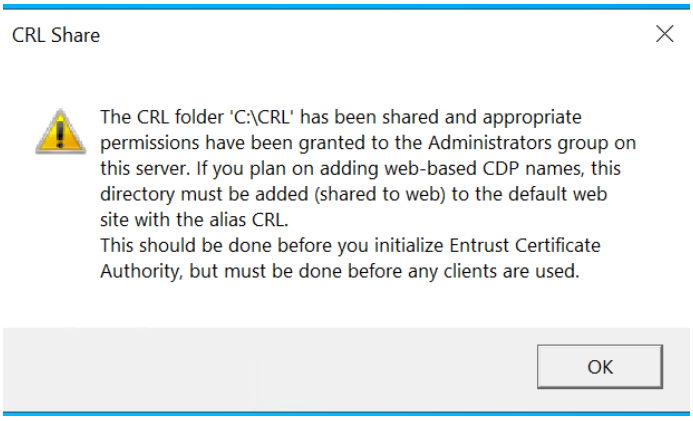


40. In the **CA Certificate Properties** dialog, accept the default of 120 months for the CA certificate lifetime and 100% for the private key usage period, then select **Next**.



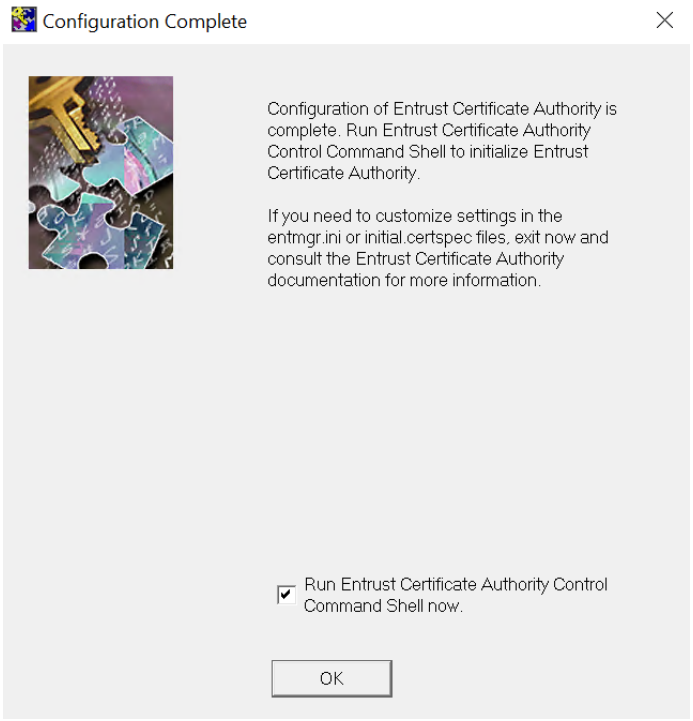
Consult your security policy of your organization about recommendations for CA lifetime.

The **CRL Share Warning** dialog appears.



41. Select **OK**.

    The **Configuration Complete** dialog appears.



42. To initialize the CA, select **Run Certificate Authority Command Shell now**, and then select **OK**.

    The Certificate Authority Control Command Shell (`entsh`) launches, and starts the CA initialization process.

    You will have the option to initialize the CA later by running the `init` command from the `entsh` command window.

43. Provide the password for the HSM PKCS11 user that you created when you

installed and initialized the HSM using the tools provided by the HSM.

44. Enter and confirm passwords for all Master users and the First Officer. These are required later during testing. For example:

```
Starting First-Time Initialization...

A Hardware Security Module (HSM) will be used for the CA key:
    nCipher Corp. Ltd  SN : edb3d45a28e5a6b2
    The HSM requires a password.

Enter password for CA hardware security module (HSM):
Enter new password for Master1:
Confirm new password for Master1:
Enter new password for Master2:
Confirm new password for Master2:
Enter new password for Master3:
Confirm new password for Master3:
Enter new password for First Officer:
Confirm new password for First Officer:

Initialization starting; creating ca keys...
Initialization complete.
Starting the services...
Creating CA profile...
Creating First Officer profile...
You are logged in to Entrust Certificate Authority Control Command Shell.
Performing database backup...
SUCCESS: Full backup completed successfully.
Press return to exit
```

45. Close any open windows or dialogs.

Chapter 6. Test the integration

6.1. Initialize Entrust Certificate Authority

If you did not initialize the Certificate Authority at the end of the configuration process:

1. Open a Windows command terminal.
2. Initialize Certificate Authority:

```
% cd C:\Program Files\Entrust\Certificate Authority\bin
% entsh.exe -e "source \"C:\Program Files\Entrust\Certificate Authority\bin\FirstTimeInit.tcl\""
```

6.2. Launch the Entrust Certificate Authority Shell

To launch the Entrust Certificate Authority Shell:

1. Open a Windows command terminal.
2. Open an Entrust Shell:

```
% cd C:/Program Files/Entrust/Certificate Authority/bin
% entsh.exe
```

Further commands during testing are executed inside the Entrust Shell.

6.3. Verify the in-memory CA key cache

To verify the in-memory CA key cache:

1. In the Entrust Shell:

```
entsh$ ca key show-cache
Master User Name: Master1
Password:
**** In Memory CA cache ****
Record Status Legend:
  C = current key
  H = key on hold
  A = non-current key
  X = revoked or expired non-current key has been obsoleted
  HWV1 = hardware key PKCS11 V1 *** NOT SUPPORTED ***
  HWV2 = hardware key PKCS11 V2
  SW = software key

-----------------------------------------------------

Internal key index:          1
```

```
CA certificate issued by:     ou=CAentry,dc=entrustsm,dc=local
serial number:                00CA3C0FCE0615F924AD191620ED4B67E0
current CA certificate:       Y
CA certificate issue date:    Thu Oct 10 04:14:04 2024
CA certificate expire date:   Tue Oct 10 04:44:04 2034
subject key identifier:       ADD12C617C66FDFFD54F080FD70CFDF4EC70CCA8
private key active:           Y
private key expired:          N
certificate expired:          N
certificate revoked:          N
revocation details:           N/A
key:                          RSA-2048
global signing policy:        RSA-SHA256 (sha256WithRSAEncryption)
record status in database:    C HWV2
migrated:                     N
hardware load error:          N
hardware CKA_ID:              LOBrpuJUJRraNabR02/MTLcX5kE=
hardware status: Loaded >> 'nCipher Corp. Ltd  SN : edb3d45a28e5a6b2 SLOT : 761406614'.

-----------------------------------------------------
**** End of In Memory CA cache ****
```

6.4. Verify the hardware information

To verify the hardware information:

1. In the Entrust Shell:

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key show-cahw -type all

EAC is not enabled. There is no associated cryptographic hardware for EAC.


**** Hardware Information ****

-----------------------------------------------------

Name:
nCipher Corp. Ltd  SN : b02xxxxxxxxxxxxxxxx19e SLOT : 761406614

Has current X.509 CA key: Y
Load Status:              hardware loaded ok
Uses Password:            Y
DB protection HW:         N
In use for X.509 CA keys: Y
In use for EAC keys:      N
ECDSA style:              4 (use raw digest padded to large digest size)

-----------------------------------------------------

Name:
nCipher Corp. Ltd  SN : EMPTY_SN SLOT : 761406613

Has current X.509 CA key: N
Load Status:              hardware loaded ok
Uses Password:            N
DB protection HW:         N
In use for X.509 CA keys: N
In use for EAC keys:      N
ECDSA style:              4 (use raw digest padded to large digest size)

-----------------------------------------------------
```

```
**** End of Hardware Information ****
```

6.5. Import the CA key pair from software to hardware

To import the CA key pair from software to the HSM (from software to hardware):

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key update
```

This prompts you to select the destination for the new CA key.

Select the **nCipher** slot as the destination for the new CA key. For example:

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key update

Select the destination for the new CA key.
Choose one of:
1. Software
2. nCipher Corp. Ltd  SN : EMPTY_SN SLOT : 761406613
3. nCipher Corp. Ltd  SN : edb3d45a28e5a6b2 SLOT : 761406614
4. Cancel operation
> 3
If the cluster is running it will be stopped and the CA key updated.
Do you wish to continue (y/n) ? [y] y
Checking cluster status...

Stopping cluster...

100% complete. Estimated time remaining -:-:- \

CA key and certificate successfully updated.
Recovering CA profile...
Starting cluster...


CA profile successfully recovered.

It is recommended that all revocation lists be re-issued. This can be done later with the 'rl issue' command. Re-
issue revocation lists
now (y/n) ? [y] y

Issuing CRLs, please wait ...


1 CRL(s) were issued.
1 ARL(s) were issued.
1 combined CRL(s) were issued.



Publishing CRLs, please wait ...
```

After you have moved the CA key to the HSM and have finished updating it, a message about the CA profile being successfully recovered appears.

6.6. Export the CA key pair from hardware to software

To export the Entrust CA key pair from the HSM to software (from hardware to software), use the Entrust Shell:

```
ou=CAentry,dc=entrustsm,dc=local.Master1 $ ca key update
Select the destination for the new CA key.
Choose one of:
1. Software
2. nCipher Corp. Ltd  SN : EMPTY_SN SLOT : 761406613
3. nCipher Corp. Ltd  SN : edb3d45a28e5a6b2 SLOT : 761406614
4. Cancel operation
> 1
If the cluster is running it will be stopped and the CA key updated.
Do you wish to continue (y/n) ? [y] y
Checking cluster status...

Stopping cluster...

100% complete. Estimated time remaining -:-:- -

CA key and certificate successfully updated.
Recovering CA profile...
Starting cluster...


CA profile successfully recovered.

It is recommended that all revocation lists be re-issued. This can be done later with the 'rl issue' command. Re-issue revocation lists now (y/n) ? [y] y

Issuing CRLs, please wait ...


1 CRL(s) were issued.
1 ARL(s) were issued.
1 combined CRL(s) were issued.



Publishing CRLs, please wait ...
```

After you have finished updating the CA key, its export to software is complete.

6.7. Back up Security World files

To back up Security World files:

1. Back up the `C:\ProgramData\nCipher\Key Management Data\local` directory.

   Such a backup of Security World files must be performed after any new key generation or Security World administration activities.

2. Store the backup files according to your organization's disaster recovery instructions.

Chapter 7. Troubleshooting

7.1. (-8973) Could not connect to the Entrust Certificate Authority service. Certificate Authority service may not be running

The Entrust service is not running in the Entrust Authority Master Control shell (`entsh$`).

Resolution:

1. Open the Master Control shell (`entsh$`).
2. Log in with `Master1`.
3. Run `Service Start`.

7.2. Error encountered querying CA hardware

When you are configuring Certificate Authority, you see the following message:

```
Are you using a hardware device for the CA keys (y/n) ? [n] y

Enter the pathname for the CryptokiLibrary.
[/opt/nfast/toolkits/pkcs11/libcknfast.so] >

Error encountered querying CA hardware.
```

Resolution:

1. Make sure you have an operator card set in the HSM.
2. Once that is in place, the script should be able to see the HSM.

7.3. (-77) Problem reported with crypto hardware

When you are initializing Certificate Authority, you see the following message:

```
Initialization starting; creating ca keys...
(-77) Problem reported with crypto hardware.
GenerateKeyPairX509
Press return to exit
```

Resolution:

1. Make sure that the following variable in the `cnkfastrc` file is set to `1`.

```
CKNFAST_LOADSHARING=1
```

7.4. (-2229) An error occurred. Check the service status and manager logs for details

This is a timeout issue.

Resolution:

1. Log in to `entsh$`.
2. Run `service status`.
3. If the service is shown as `down`, start it by running `service start`.

If you are using an nShield Edge, see nShield Edge pre-configuration.

7.5. HSM logs show missing algorithms errors that are not configured by Certificate Authority during startup

Certificate Authority performs a FIPS Self-Test where many algorithms and functions beyond those explicitly configured to be used once operational. These tests are required by FIPS 140 conformance.

Resolution:

1. If algorithms are not available during self-test, Certificate Authority treats this as informational only.
2. FIPS Self Tests HSM log errors do NOT stop Certificate Authority startup.

7.6. No Hardware Device Found

During the configuration of Entrust Certificate Authority, the message "No Hardware Device Found" pops up every time, even if the right library is selected.

Resolution:

1. Make sure the `entconfig.ini` and `entrust.ini` both have the correct PKCS#11 library setting.

2. Ensure that any HSM service is running.

7.7. (-2684) General hardware error

HSM Service is not available.

Resolution: Ensure that any HSM service is running and responding.

7.8. nShield Edge Cluster Status

Ensure that the `entMgr.ini` file is as defined in nShield Edge pre-configuration.

The nShield Edge exhibits slower service startup times with respect to operations, which is to be expected. When checking the cluster status after initial set-up, you may encounter services with a "down" status or an "unknown" cluster status. To ensure proper initialization of the cluster and services, Entrust recommends allowing a few minutes for the system to complete the process. After sufficient time has passed, the services and cluster should display the correct status.

In some cases you will need to start the cluster manually. For example:

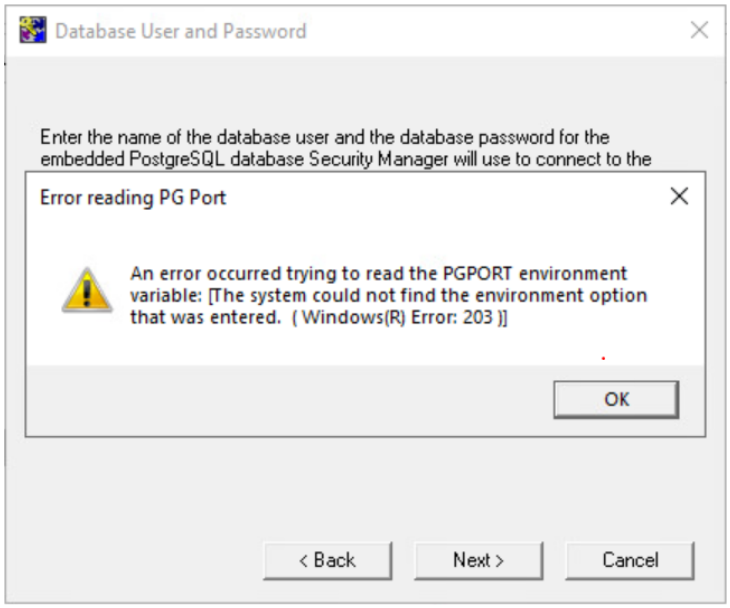
```
entsh$ cluster status
ca_wide_entry   disabled
localhost       enabled     quiescent **LOCAL**

entsh$ cluster start
Starting cluster...

entsh$ cluster status
ca_wide_entry   enabled
localhost       enabled     quiescent **LOCAL*
```

For more information regarding the cluster status, refer to *s 10.0 Cluster Management Guide Issue 4.0*, which is available on the Entrust TrustedCare Portal.

7.9. pg_port error



Resolution: Install and configure PostgreSQL before you configure Certificate Authority.

Chapter 8. Additional resources and related products

8.1. nShield Connect

8.2. nShield as a Service

8.3. Entrust products

8.4. nShield product documentation