Entrust Cryptographic Security Platform PKI Hub

nShield® HSM Integration Guide

2026-10-14

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configuration . . . 1
    1.2. Supported nShield hardware and software versions . . . 1
    1.3. Requirements . . . 2
2. Deploy Entrust Cryptographic Security Platform PKI Hub . . . 3
3. Install and configure the Entrust nShield HSM . . . 4
    3.1. Install the Entrust nShield HSM . . . 4
    3.2. Install the Entrust nShield Security World Software and create the Security World . . . 4
    3.3. Edit the configuration files . . . 5
    3.4. Create the OCS . . . 6
4. Integrate the Entrust Cryptographic Security Platform PKI Hub and the Entrust nShield HSM . . . 7
    4.1. Make the Entrust Cryptographic Security Platform PKI Hub server a client of the HSM . . . 7
    4.2. Configure the Entrust Cryptographic Security Platform PKI Hub . . . 7
5. Test the integration . . . 11
6. Additional resources and related products . . . 13
    6.1. nShield as a Service . . . 13
    6.2. KeyControl . . . 13
    6.3. KeyControl as a Service . . . 13
    6.4. Entrust products . . . 13
    6.5. nShield product documentation . . . 13

Chapter 1. Introduction

The Entrust Cryptographic Security Platform PKI Hub is a versatile virtual appliance that streamlines deployment of the following Entrust solutions across a range of environments: Certificate Authority, CA Gateway, Certificate Enrollment Gateway, Certificate Hub, Timestamping Authority, and Validation Authority. The Entrust nShield Hardware Security Module (HSM) securely stores and manages encryption keys. This document describes how to integrate the HSM with PKI Hub to add security to your PKI.

The HSM is available as an appliance or as nShield as a Service (nSaaS). Throughout this guide, the term HSM refers to nShield Solo, nShield Connect, and nShield Edge products.

1.1. Product configuration

Entrust tested the integration with the following versions:

Product	Version
Entrust Cryptographic Security Platform	v1.5
Entrust Cryptographic Security Platform PKI Hub	v1.6.0
Security World (Embedded in the product)	v13.9.0
Security World Client	v13.6.18 (LTS8) / v13.9.6 (STS6)
PostgreSQL	15.17 (Deployed on a Red Hat 9 Linux server)
VMWare vSphere	9.0

1.2. Supported nShield hardware and software versions

Entrust tested the integration with the following nShield hardware and software versions. The integration was tested using OCS protection. Module-protected keys are not supported in Entrust Certificate Authority v10.0 and later versions.

When using a FIPS 140 Level 3 Security World, you must present the OCS card in the front slot of the HSM.

Product	Firmware	Netimage	FIPS 140 Level 3
Connect XC	13.8.5	13.9.6	No
Connect XC	12.72.4 (FIPS 140-2 certified)	13.6.18	Yes
nShield 5c	13.8.6	13.9.6	No
nShield 5c	13.4.5 (FIPS 140-3 certified)	13.6.18	Yes

1.3. Requirements

To integrate the HSM and PKI Hub, you require:

- A dedicated virtual appliance for the installation.
- A dedicated server for hosting a PostgreSQL database and the Entrust nShield key management data.
- Access to the Entrust TrustedCare Portal.

Familiarize yourself with:

- The Entrust Cryptographic Security Platform PKI Hub documentation.
- The nShield documentation.
- Your organizational Certificate Policy, 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 key protection method: Module, Softcard, or OCS. (Only OCS is supported).
  - The level of compliance for the Security World, FIPS 140 Level 3.

    When using a FIPS 140 Level 3 Security World, you must present the OCS card in the front slot of the HSM.

  - Key attributes such as key size and time-out are required for auditing key usage.

Chapter 2. Deploy Entrust Cryptographic Security Platform PKI Hub

For this integration, the Entrust Cryptographic Security Platform PKI Hub was deployed from an ISO image in a virtual environment. A single node was deployed. The required PostgreSQL database was deployed in a virtual Red Hat 9 Linux environment.

The complete instructions are available in the Entrust Cryptographic Security Platform PKI Hub documentation.

Chapter 3. Install and configure the Entrust nShield HSM

This section applies to on-premises applications. In nSaaS applications, the Entrust PKI Hub obtains key management data as defined by the nSaaS service.

Deploy a Linux server and install the Security World software on it. Configure this server as a client of the HSM, then create a Security World and OCS.

The Entrust Cryptographic Security Platform PKI Hub utilizes the key management data from this server.

3.1. Install the Entrust nShield HSM

Install the nShield Connect HSM locally, remotely, or remotely using the serial console. Condensed instructions are available in the following Entrust nShield Support articles.

- How To: Locally Set up a new or replacement nShield Connect.
- How To: Remotely Setup a new or replacement nShield Connect.
- How To: Remotely Setup 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.

The complete instruction set is available at nShield Hardware Install and Setup Guides.

For detailed instructions, see the nShield documentation.

3.2. Install the Entrust nShield Security World Software and create the Security World

This section applies to the server on which the Entrust nShield HSM infrastructure is deployed.

1. Install the Security World software. For detailed instructions, see the nShield documentation.
2. Add the Security World utilities path to the system path. This path is typically `/opt/nfast/bin`.

3. Open firewall port 9004 for the Entrust nShield HSM connections.
4. If using remote administration, open firewall port 9005 for the Entrust nShield Trusted Verification Device (TVD).

When using a FIPS 140 Level 3 Security World, you cannot use a TVD. The OCS card must be presented in the front slot of the HSM.

5. Configure the server as a client of the Entrust nShield HSM.
6. Open a command window and run the following command to confirm that the Entrust nShield HSM is **operational**.

```
root@dev-ubuntu:~# enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.9.6
...
Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        92C8-8591-52EB
 mode                 operational
 version              13.8.6
 ...
```

7. Create your Security World or copy an existing one. Follow your organization's security policy when doing so.

ACS cards cannot be duplicated after the Security World is created. You may want to create extras according to your organization's security policy.

8. Confirm the Security World is `usable`.

```
root@dev-ubuntu:~# nfkminfo
World
 generation  2
 state       0x3737000c Initialised Usable ...
 ...
Module #1
 generation 2
 state      0x2 Usable
```

3.3. Edit the configuration files

This section applies to the server on which the Entrust nShield HSM infrastructure is deployed.

1. Edit the configuration file `/opt/nfast/cknfastrc`, adding the lines shown below. Set the file permissions to **read and execute** for all users.

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
CKNFAST_LOADSHARING=1
```

2. Edit the configuration file `/opt/nfast/kmdata/config/cardlist`. Add the serial numbers of the remote-administration-ready OCS smart cards or a wildcard.
3. Restart the Security World software.

```
% sudo /opt/nfast/sbin/init.d-ncipher restart
```

3.4. Create the OCS

OCS cards are presented to the HSM's physical smart card reader. For more information about OCS use, properties, and k-of-N values, see the nShield documentation.

If you have an existing Entrust nShield HSM infrastructure, you can use an existing OCS (k=1) that corresponds to your world or you can create a new one. The quorum (k) in k-of-N must be 1 for this application.

If you create a new OCS, follow your organization's security policy and set k=1.

OCS cards cannot be duplicated after they are created. You may want to create extras according to your organization's security policy. When using a FIPS 140 Level 3 Security World, you cannot use a TVD. The OCS card must be presented in the front slot of the HSM.

Chapter 4. Integrate the Entrust Cryptographic Security Platform PKI Hub and the Entrust nShield HSM

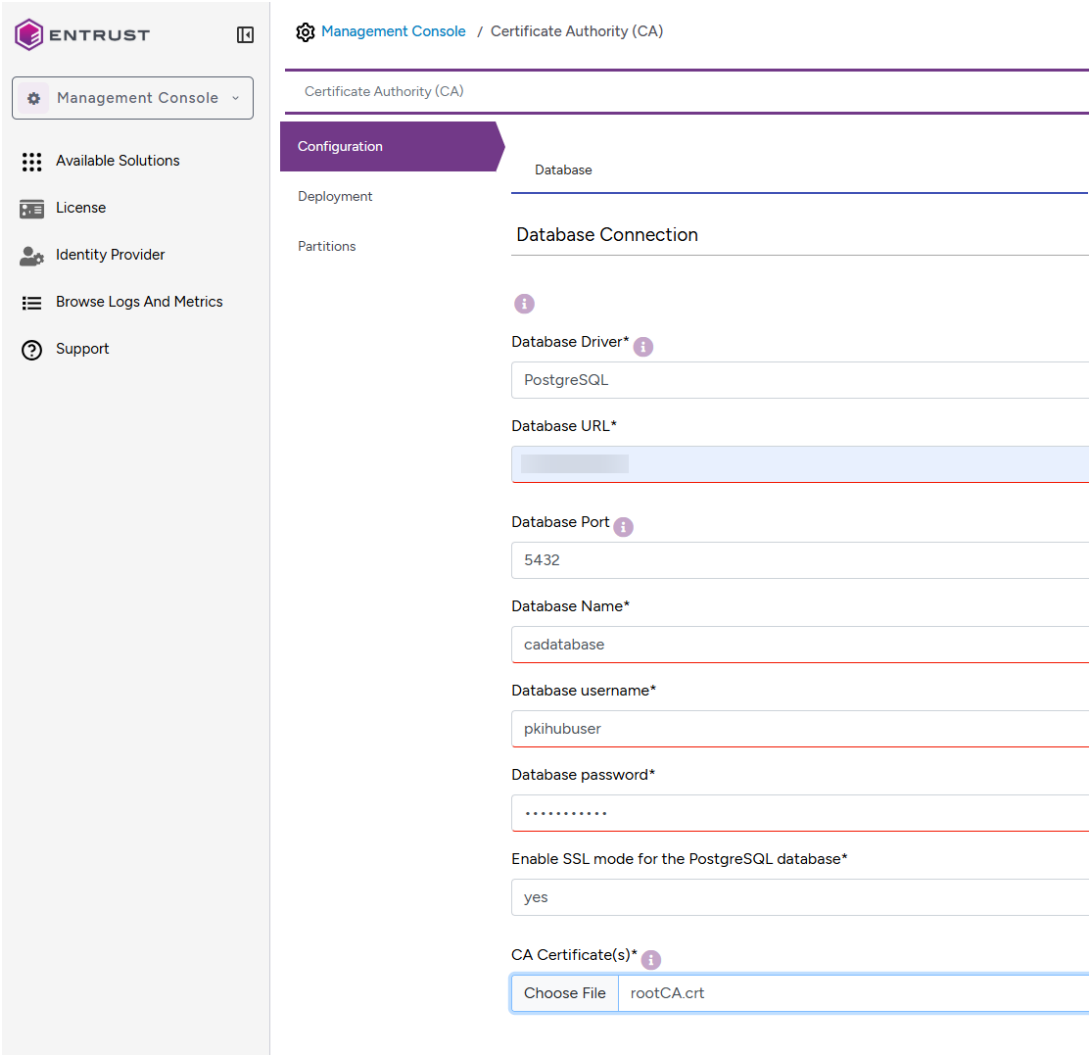
4.1. Make the Entrust Cryptographic Security Platform PKI Hub server a client of the HSM

1. Using the HSM front panel, add the IP address of the Entrust Cryptographic Security Platform PKI Hub server as a client of the HSM.
2. Present the OCS card from Install and configure the Entrust nShield HSM to the HSM through the front panel card reader.

4.2. Configure the Entrust Cryptographic Security Platform PKI Hub

1. Log in to the Entrust Cryptographic Security Platform PKI Hub Management Console web interface as explained in *Starting up the Management Console* in the Cryptographic Security Platform PKI Hub documentation.
2. In the content pane, under **Certificate Authorities**, select **Manage Solution**.
3. Leave **Import configuration** set to its default off position.
4. Set **Enable Advanced Configuration** to **Yes**.
5. Select **Next**.
6. In the **Database** tab, enter the database information described in Deploy Entrust Cryptographic Security Platform PKI Hub, then select **Next**.

   You must create a separate database for the solution. Do not use the same database used to deploy the PKI Hub cluster. For example:



7. In the **HSM** tab, enter the HSM information.
   a. For **Vendor**: Select **nShield**.
   b. For **OCS (Operator Card Set) passphrase**: Enter the passphrase for the OCS card being used for the integration.
   c. For **The nShield kmdata tar file**:

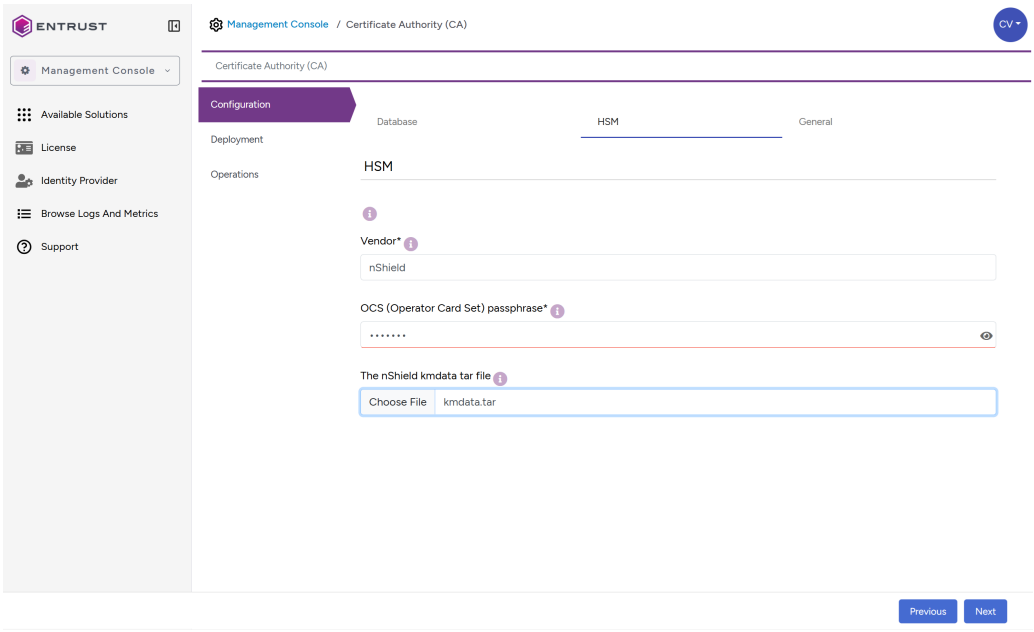
      Create a tar file containing the HSM's Key Management data directory (`kmdata`) and upload it here. The file should contain the OCS card files created for the integration. Run this shell command on the server where the HSM was configured and the `kmdata` directory is located.

      ```
      % sudo tar -cf x.tar -C /opt/nfast kmdata.
      ```

      Then copy `kmdata.tar` to your host so you can upload it here.

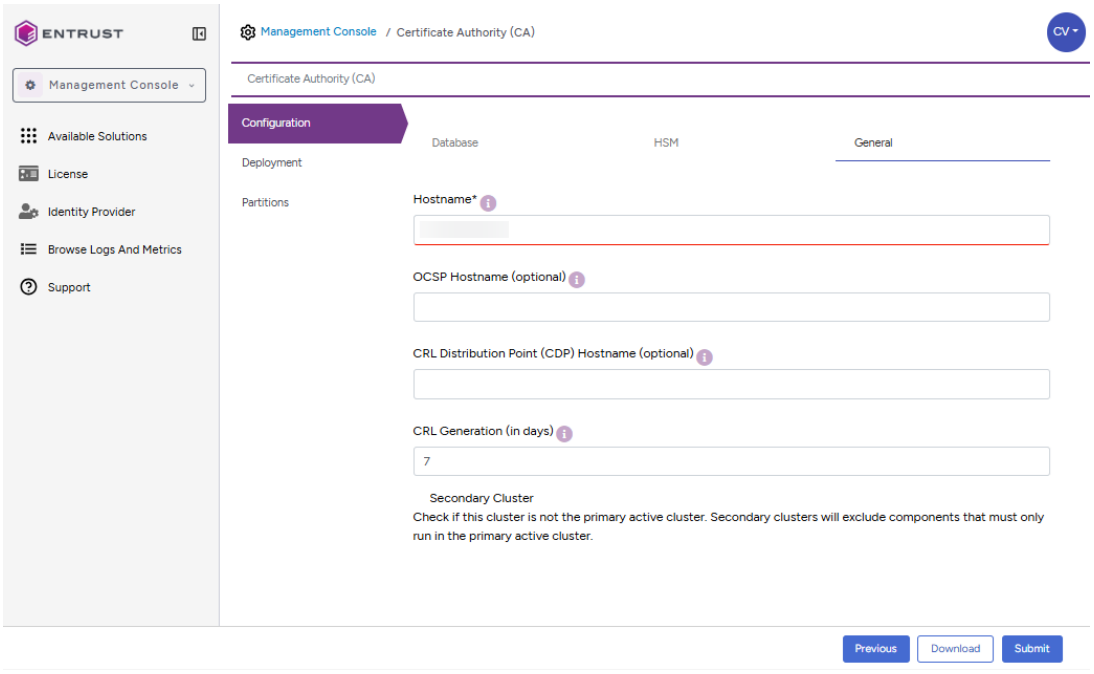
   d. Select **Next**.

For example:

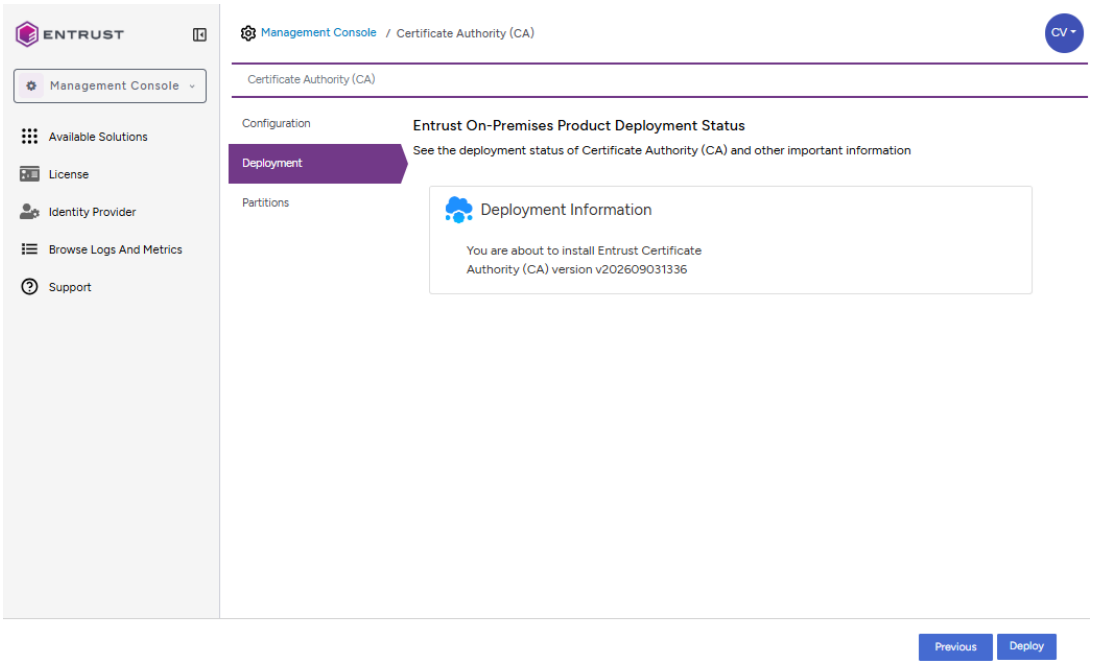


8. In the **General** tab, enter the Entrust Cryptographic Security Platform PKI Hub hostname or IP.

   For example:

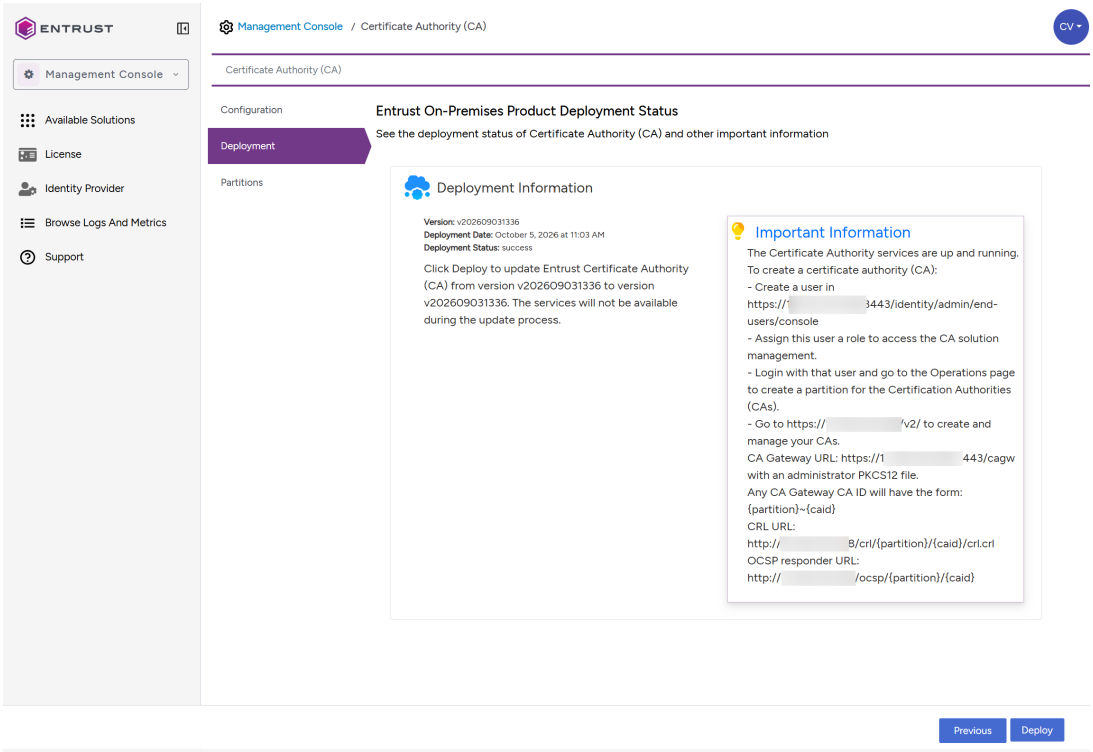


9. Select **Submit**. If everything is accepted, the console displays the **Deployment** page.



10. Select **Deploy**, then, in the **Confirmation** pop-up window, select **Yes**. After a few minutes, the integration with the Entrust nShield HSM is complete.

    For example:



Chapter 5. Test the integration

This test validates the key created in the HSM during Integrate the Entrust Cryptographic Security Platform PKI Hub and the Entrust nShield HSM.

1. Log in to the Entrust Cryptographic Security Platform PKI Hub Management Console web interface.
2. In the content pane, under **Certificate Authorities**, select **Manage Solution**.
3. Select the download arrow icon to the right of **Export Configuration**. The compressed file (`pkihub-configuration.zip`) downloads to your computer.
4. Extract the compressed file, `pkihub-configuration.zip`.
5. Navigate to `Downloads\pkihub-configuration` to find `kmdata.tar`.
6. Extract the `kmdata.tar` archive.

   ```
   % tar -xvf kmdata.tar
   ```

   The `kmdata/local` folder now contains the HSM files.

   The `key_ncore_pkihub-attila-wrapping-key` file is the key blob for the key created in the Entrust nShield HSM.

7. To validate the key, copy the key blob to an HSM client using the same Security World and place it in `/opt/nfast/kmdata/local/`.
8. Run the following commands and note the key name.

   ```
   % nfkminfo -k

   Key list - 1 keys
    AppName ncore               Ident pkihub-attila-wrapping-key


   % rocs
   `rocs' key recovery tool
   Useful commands: `help', `help intro', `quit'.
   rocs> list keys
     No. Name                           App   Protected by
       1 Id: pkihub-attila-wrapping-key ncore testOCS

   rocs> exit
   ```

9. Verify the key.

   ```
   % nfkmverify ncore pkihub-attila-wrapping-key

   ** [Security world] **
       Ciphersuite: DLf3072s256mAEScSP800131Ar1
       128-bit security level
       7 Administrator Card(s)
   ```

```
    (NOT IN ANY SLOT of an attached module)
    HKNSO b5cb518930e8dd1fea1bd8a3e99347b598382d85
    Cardset recovery ENABLED
    Passphrase recovery disabled
    Common Criteria CMTS 419221-5 disabled
    Strict FIPS 140-2 level 3 (does not improve security) disabled
    SEE application non-volatile storage ENABLED
    real time clock setting ENABLED
    SEE debugging ENABLED
    SEE debugging restricted
    Foreign Token Open authorization ENABLED
    Generating module ESN 92C8-8591-52EB NOT ATTACHED to this host

---


** [Application key ncore pkihub-attila-wrapping-key] **
    [Not named]
    Useable by HOST applications
    Cardset protected: 1/6 ephemeral [0s `testOCS']
    Cardset hash 321b143185fc939504893270ed821ba4ed38319a
     (Currently in Module #1 Slot #2: Card #6)
    Key useable INDEFINITELY (after card loading)
    Recovery ENABLED
    Type HMACSHA256 256 bits
    Key may be used for: GENERATING or verifying message authentication codes
    Generating module ESN 201E-03E0-D947 currently #1 (in same incarnation)
    nCore hash 8eab3b67885df5fdfb8b1a05300ea34d366afe55
    Public half is ABSENT

Verification successful, confirm details above.  1 key verified.
```

10. Delete this key blob from the HSM client or server. The key remains in the Entrust PKI Hub.

Chapter 6. Additional resources and related products

6.1. nShield as a Service

6.2. KeyControl

6.3. KeyControl as a Service

6.4. Entrust products

6.5. nShield product documentation