Entrust Cryptographic Security Platform PKI Hub

nShield® HSM Integration Guide

2025-11-27

Table of Contents

Chapter 1. Introduction

The Entrust Cryptographic Security Platform PKI Hub is a versatile and robust virtual appliance that streamlines and simplifies deployment across various environments of the following Entrust solutions: Certificate Authority, CA Gateway, Certificate Enrollment Gateway, Certificate Hub, Timestamping Authority, and Validation Authority. 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). 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	v1.2
Entrust Cryptographic Security Platform PKI Hub	v1.3.0
Security World	v13.9.0 (Embedded in the product)
PostgreSQL	15.14 (Deployed on a Red Hat 9 Linux server)
VMWare vSphere	8.0

1.2. Supported nShield hardware and software versions

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

Product	Firmware	Netimage
Connect XC	13.8.0	13.9.0
nShield 5c	13.8.0	13.9.0

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 keys protection method: Module, Softcard, or OCS. (Only OCS is supported).
  - The level of compliance for the Security World, FIPS 140 Level 3.
  - Key attributes such as key size, time-out, or needed for auditing key usage.

Chapter 2. Deploy Entrust Cryptographic Security Platform PKI Hub

For the purpose of this integration, the Entrust Cryptographic Security Platform PKI Hub was deployed from iso 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 instruction set is 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 gets the key management data as defined by the nSaaS service.

Deploy a Linux server and install in it the security world software. Make this server a client of the HSM and create a 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 via 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 v13.9.0 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 deployed where Entrust nShield HSM infrastructure exists.

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

```
root@dev-ubuntu:~# enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number
 mode                 operational
 version              13.9.0
...
Module #1:
 enquiry reply flags  UnprivOnly
 enquiry reply level  Six
 serial number        92C8-8591-52EB
 mode                 operational
 version              13.8.0
 ...
```

7. Create your Security World or copy an existing one. Follow your organization's security policy for this.

ACS cards cannot be duplicated after the Security World is created. You may want to create extras per your organization 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 where the Entrust nShield HSM infrastructure exists.

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

```
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 wild card.
3. Restart the Security World software.

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

3.4. Create the OCS

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

For an existing Entrust nShield HSM infrastructure, you have the choice of using an existing OCS (k=1) corresponding to your world, or create a new one. The quorum k of k-of-N must be 1 for this application.

Otherwise, create an OCS card set following your organization's security policy, with k=1.

OCS cards cannot be duplicated after they are created. You may want to create extras per your organization security policy.

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

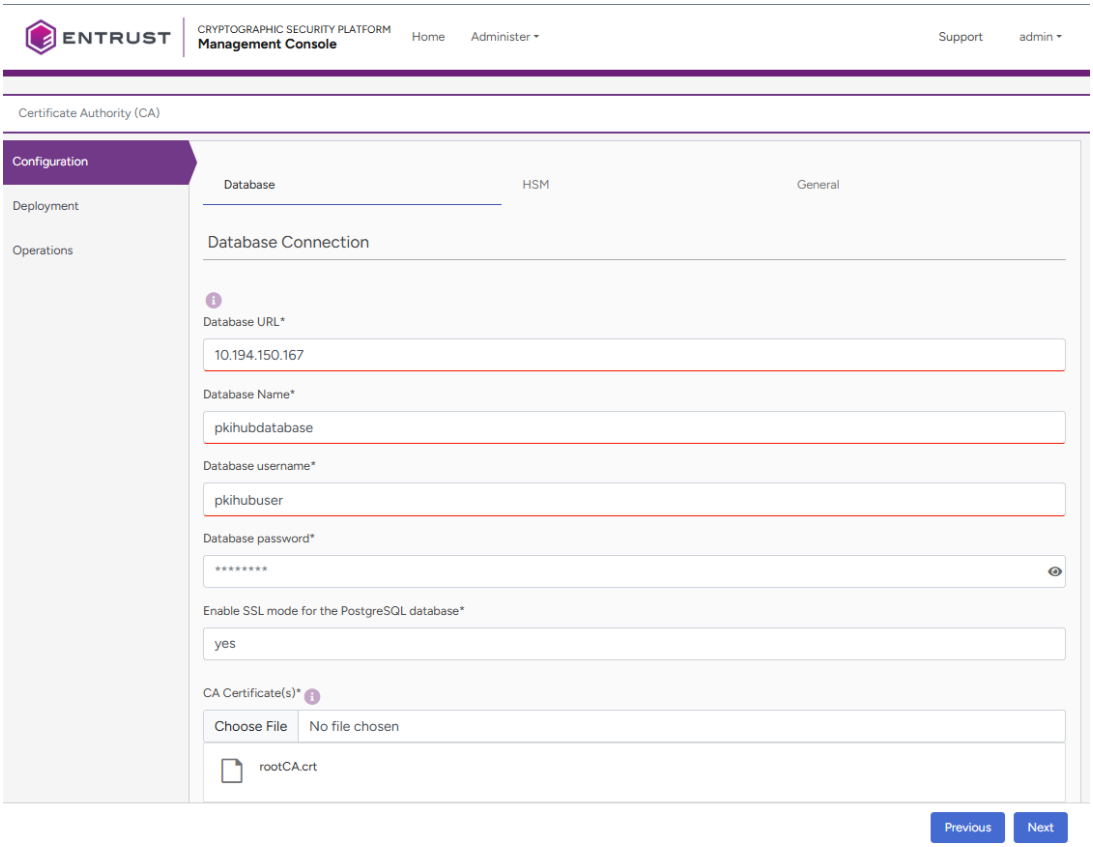
4.1. Make the Entrust Cryptographic Security Platform PKI Hub server a client of the HSM

1. Using the HSM front panel, add the IP 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 into the Entrust Cryptographic Security Platform PKI Hub Management Console web GUI 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 the **Import configuration** and **Enable Advanced Configuration** toggle switches in the default off position. Then select **Next**.
4. In the **Database** tab, enter the database information from Deploy Entrust Cryptographic Security Platform PKI Hub. Then select **Next**.

   For example:



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

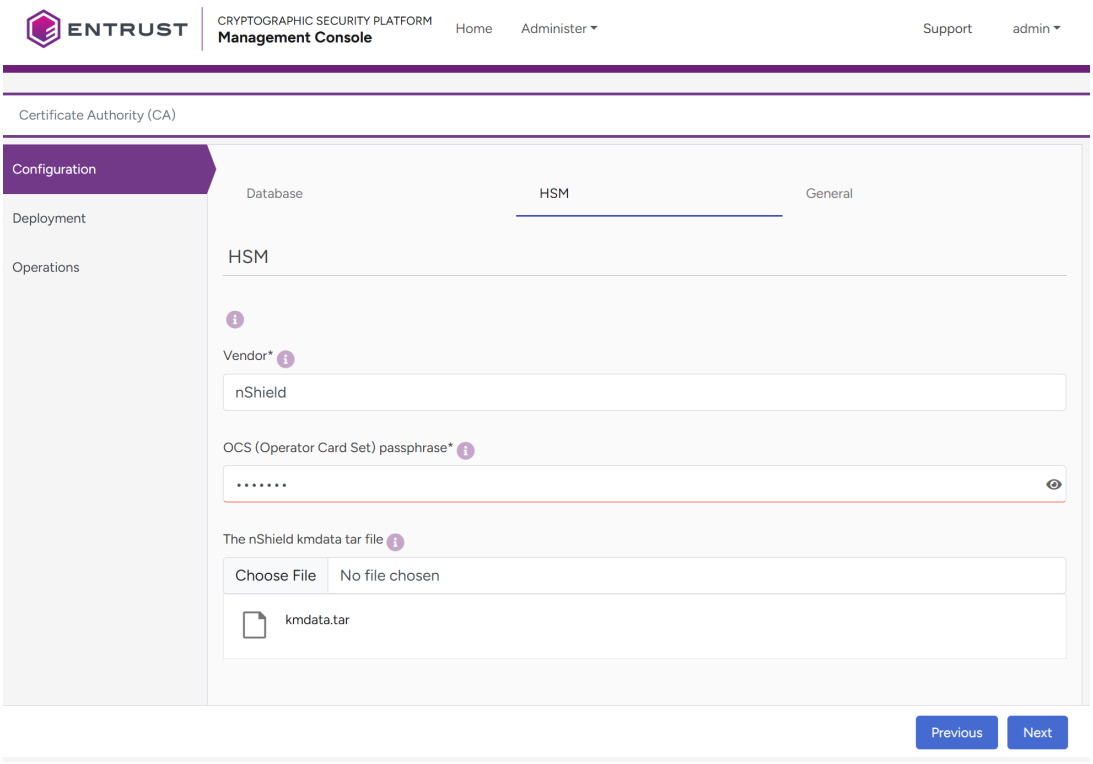
   You need to create a tar file containing the Key Management data directory (`kmdata`) of the HSM and supply that file here. Run this shell command in the server with the `kmdata` directory where the HSM was configured.

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

   Then copy the `kmdata.tar` to your host so you can upload it here. .. Then select **Next**.

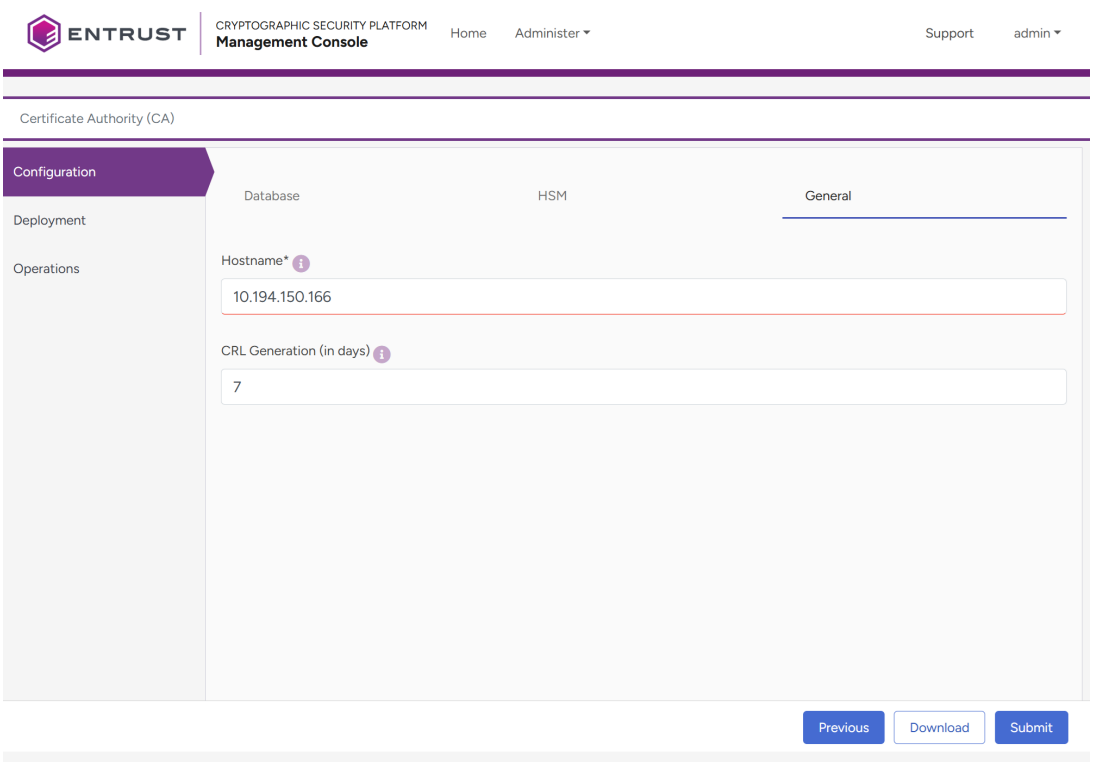
   +

   For example:

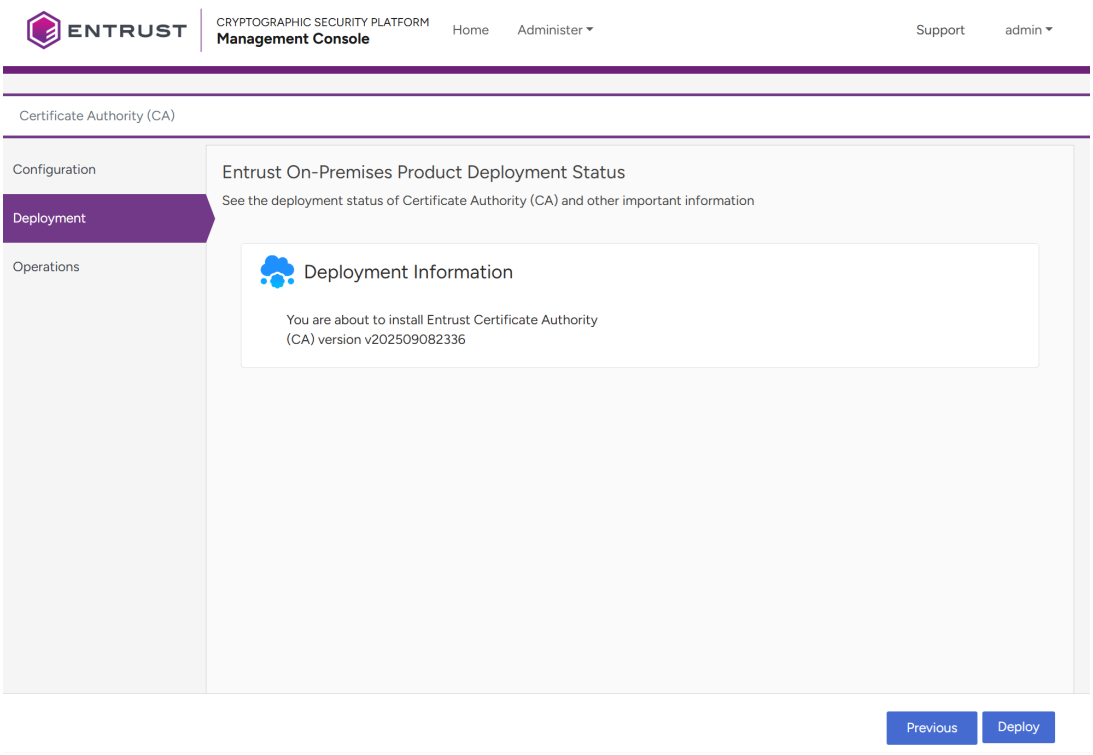


6. In the **General** tab, enter the Entrust Cryptographic Security Platform PKI Hub hostname or IP.

   For example:

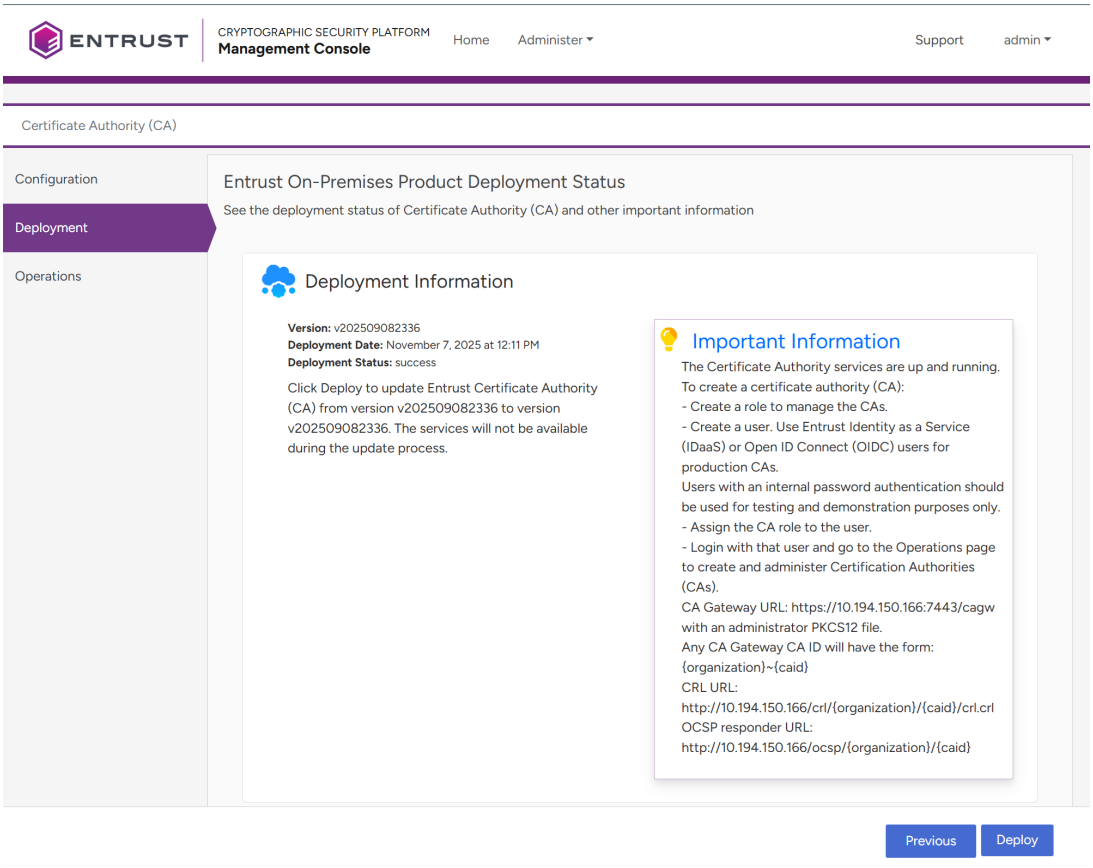


7. Select **Submit**. If everything is accepted, it should take you to the **Deployment** page.



8. Select **Deploy**. In the **Confirmation** pop-up window select **Yes**. After a few minutes, the configuration with the Entrust nShield HSM completes.

   For example:



Chapter 5. Test the integration

This test consists of validating the key created in the HSM in Integrate the Entrust Cryptographic Security Platform PKI Hub and the Entrust nShield HSM.

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

   The `kmdata/local` folder with the HSM files are now available

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

   - Notice the `key_ncore_⋯` file, that is, `key_ncore_pkihub-attila-wrapping-key`. This file is the key blob corresponding to the key created in the Entrust nShield HSM.
7. For the purpose of validating the key, copy the key blob to a HSM client using the same world and place it in the folder `/opt/nfast/kmdata/local/`.
8. Execute the following commands. Notice 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.

   ```
   ** [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 currently #1
    Generating module has since been ERASED AND REPROGRAMMED

---


** [Application key ncore pkihub-attila-wrapping-key] **
    [Not named]
    Useable by HOST applications
    Cardset protected: 1/1 PERSISTENT [0s `testOCS']
    Cardset hash ba061036ffd4bb52c7403bc9fb5ff50bbe6e6cfe
     (Currently in Module #1 Slot #2: Card #1)
    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 92C8-8591-52EB currently #1 (in same incarnation)
    nCore hash c6c96634f71f155050d624704f71053753c66c74
    Public half is ABSENT

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

10. Delete this key blob from the HSM client or server. It 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