# Venafi TLS Protect Datacenter

## nShield® HSM Integration Guide

**21 Nov 2023**

# Contents

# 1. Introduction

This document describes how to integrate the Venafi TLS Protect Datacenter with the Entrust nShield hardware security module (HSM) as a Root of Trust for storage encryption, to protect the private keys and meet FIPS 140 Level 2 or Level 3.

## 1.1. Product configurations

Entrust has successfully tested nShield HSM integration with Venafi TLS Protect Datacenter in the following configurations:

| Product | Version |
|---|---|
| Venafi TLS Protect Datacenter | 23.3.0.3410 |
| Base OS | Windows Server 2016 |

## 1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

### 1.2.1. Connect XC

| Security World Software | Firmware | Image | OCS | Softcard | Module |
|---|---|---|---|---|---|
| 12.80.4 | 12.50.11 (FIPS Certified) | 12.80.4 | ✓ | ✓ | ✓ |
| 12.80.4 | 12.72.1 (FIPS Certified) | 12.80.5 | ✓ | ✓ | ✓ |
| 13.3.2 | 12.72.1 (FIPS Certified) | 12.80.5 | ✓ | ✓ | ✓ |

### 1.2.2. nShield 5c

| Security World Software | Firmware | Image | OCS | Softcard | Module |
|---|---|---|---|---|---|
| 13.3.2 | 13.2.2 (FIPS Pending) | 13.3.2 | ✓ | ✓ | ✓ |

## 1.3. Supported nShield HSM functionality

| Feature | Support |
|---|---|
| Module-only key | Yes |
| OCS cards | Yes |
| Softcards | Yes |
| nSaaS | Yes |
| FIPS 140 Level 3 | Yes [1] |

[1] Keys cannot be exported when using FIPS Level 3 Security World. As a result, some Venafi integration functionality (such as HSM Central Private Key Generation) will only be supported on FIPS Level 2 Security Worlds.

## 1.4. Requirements

Familiarize yourself with:

- Venafi TLS Protect Datacenter documentation (https://docs.venafi.com).
- The nShield HSM: *Installation Guide* and *User Guide*.
- 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.

# 2. Procedures

## 2.1. Prerequisites

Ensure the following prerequisites are implemented:

1. Install the Entrust nShield HSM using the instructions in the *Installation Guide* for the HSM.
2. Install the Entrust nShield Security World Software, and configure the Security World as described in the *User Guide* for the HSM.
3. Edit the `cknfastrc` file located in `%NFAST_HOME%\cknfastrc`.
   - If using OCS or Softcard protection:

     ```
     CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness
     CKNFAST_NO_ACCELERATOR_SLOTS=1
     CKNFAST_LOADSHARING=1
     ```

   - If using Module protection:

     ```
     CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness
     CKNFAST_FAKE_ACCELERATOR_LOGIN=1
     CKNFAST_LOADSHARING=1
     ```

4. Install Venafi TLS Protect Datacenter. For more information, see the Venafi online documentation.

## 2.2. Create an HSM (Cryptoki) connector

You must setup an HSM connector before the nShield HSM functionally can be used within Venafi TLS Protect Datacenter.

To create an HSM (Cryptoki) connector:

1. Open the **Venafi Configuration Console**.
2. Select the **Connectors** node.
3. Select **Create HSM Connector** in the **Actions** panel.
4. Enter your Venafi TLS Protect Datacenter user credentials if required.
5. For **Name**, enter any name for the HSM connector.
6. For **Cryptoki Dll Path**, select **Browse** and locate the following path to the DLL file:

   `C:\Program Files\nCipher\nfast\toolkits\pkcs11\cknfast.dll`.

7. Select **Load Slots**.

8. Select a slot to use for the intended key protection type. This is the partition on the HSM where Venafi TLS Protect Datacenter will access the encryption keys.
9. For **User Type**, select the required user to access the HSM keys on the designated partition.
10. For **Pin**, enter the passphrase of the Card Set being used. If Module protection is being used, leave the pin blank.
11. Select **Verify**.

## 2.3. Enable Venafi Advanced Key Protect

Venafi Advanced Key Protect is required for Central and Remote HSM Private Key Generation. In addition, Venafi Code Signing Certificate Private Key Storage requires this feature to be enabled.

To enable Venafi Advanced Key Protect:

1. Open the **Venafi Configuration Console**.
2. Select **Enable Advanced Key Protect** in the **Actions** panel.
3. Review the information and confirm the action.
4. Restart the IIS, Venafi Platform, and Logging services:
    a. Select the **Product** node.
    b. Select **Website** and then select **Restart**.
    c. Select **Venafi Platform** and then select **Restart**.
    d. Select **Logging** and then select **Restart**.

## 2.4. Using HSM-protected encryption keys

HSM-protected AES keys can be generated to encrypt data stored in the Venafi TLS Protect Datacenter Secret Store.

To generate an AES key:

1. Open the **Venafi Configuration Console**.
2. Select the **Connectors** node.
3. Select the **HSM Connector** generated in an earlier step.
4. Select **Properties** in the **Actions** panel under **Encryption Driver**.
5. Enter your Venafi TLS Protect Datacenter user credentials if required.
6. Select **New Key**.
7. On the **Create New HSM Key** page, enter a **Name** and select a **Type** for the key.

8. Select **Create**.
9. Select **Apply**.
10. Select **OK**.
11. To list the newly created key and its protection type, open a command prompt and run the following command:

```
nfkminfo -l
```

## 2.5. HSM Central Private Key Generation

Venafi TLS Protect Datacenter uses the Entrust nShield HSM for private key generation for SSH keys and certificates.

Certificate Authority (CA) template objects are used in Venafi TLS Protect Datacenter to manage the certificate lifecycle. Creating one is a prerequisite to HSM Central Key Generation. For more information, see the Venafi online documentation.

Configure the Venafi platform policy to enable the Entrust nShield HSM for central HSM key generation:

1. Log in to admin console: `https://[IP_address_of_Venafi_TLS_Protect_Datacenter]/vedadmin`.
2. Select **Policy**.
3. Select **Certificate**.
4. Under **Other Information**, select your HSM Connector in the **Key Generation** drop-down menu.
5. Select **Save**.

Generate the certificate:

1. Select **Policy**.
2. Select **Add** > **Certificates** > **Certificate**.
3. In the **General Information** tab, enter the required information.
4. For **Management Type**, select **Provisioning** or **Enrollment**.
5. For **CSR Generation**, select **Service Generated CSR**.
6. For **Generate Key/CSR on Application**, select **No**.
7. In the **Subject DN** tab, enter the required information.
8. In the **Private Key** tab, enter the key information.

9. In the **Other Information** tab, search for the previously configured **CA Template**.
10. Select **Save**.
11. Select the newly generated certificate from the policy tree. The Certificate Status should be **OK**.
12. Select **Renew Now**.
13. After a minute, select **Refresh**. The certificate details will appear at the bottom of the screen.
14. If you selected **Provisioning** for **Management Type**, associate the certificate to the intended application object.
15. Check to see if the certificate was installed on this application server.

## 2.6. HSM Remote Private Key Generation

Venafi TLS Protect Datacenter uses the Entrust nShield HSM for private key generation on a remote machine hosting an application server.

There are many configurations possible for HSM Remote Private Key Generation. Not all were tested as part of the Venafi TLS Protect Datacenter integration testing.

Certificate Authority (CA) template objects are used in Venafi TLS Protect Datacenter to manage the certificate lifecycle. Creating one is a prerequisite to HSM Remote Key Generation. For more information, see the Venafi online documentation.

To set up a remote server and configure remote generation settings:

1. Install and configure the Entrust nShield HSM and Security World on the intended remote application server. The application server needs to be able to use the HSM to generate keys. For more information about compatible application servers, see the Venafi online documentation. See the Entrust nShield `Integration Guides` which contain integration steps for the intended application server.
2. Log in to admin console: `https://[IP_address_of_Venafi_TLS_Protect_Datacenter]/vedadmin`.
3. In the policy tree, select the application set up on the remote server.
4. In the **Remote Generation Settings**, for **Private Key Location**, select **Entrust nShield HSM**.

Generate the certificate:

1. Select **Policy**.

2. Select **Add** > **Certificates** > **Certificate**.
3. In the **General Information** tab, enter the required information.
4. For **Management Type**, select **Provisioning**.
5. For **CSR Generation**, select **Service Generated CSR**.
6. For **Generate Key/CSR on Application**, select **Yes**.
7. In the **Subject DN** tab, enter the required information.
8. In the **Private Key** tab, enter the key information.
9. In the **Other Information** tab, search for the previously configured **CA Template**.
10. Select **Save**.
11. Select the newly generated certificate from the policy tree. The Certificate Status should be **OK**.
12. In the policy tree, select the application set up on the remote server.
13. In the **Certificate** tab, for **Associated Certificate**, select the previously generated certificate.
14. Select **Save**.
15. In the policy tree, select the certificate.
16. Select **Renew Now**.
17. After a minute, select **Refresh**. The certificate details will appear at the bottom of the screen.
18. Check to see if the certificate was installed on the remote application server.
19. To list the newly created key and its protection type, open a command prompt on the remote application server and run the following command:

```
nfkminfo -l
```

## 2.7. Code signing

Venafi CodeSign Protect can store private code signing keys in the Entrust nShield HSM. This section of the document describes the basic steps used to achieve this functionality for the integration. For more detailed procedures, see the Venafi online documentation.

Certificate Authority (CA) template objects are used in Venafi TLS Protect Datacenter to manage the certificate lifecycle. Creating one is a prerequisite to CodeSign. For more information, see the Venafi online documentation.

To use an HSM for key storage, you must first enable Key Storage on the HSM Connector:

1. Open the **Venafi Configuration Console**.
2. Select the **Connectors** node.
3. Select the **HSM Component** generated in an earlier step.
4. Select **Properties** in the **Actions** panel under **Encryption Driver**.
5. Enter your Venafi TLS Protect Datacenter user credentials if required.
6. Select **Allow Key Storage**.
7. Select **Apply**.
8. Select **OK**.

To choose a code signing Administrator:

1. Open the **Venafi Configuration Console**.
2. Select the **System Roles** node.
3. Select **Add CodeSign Protect Administrator** in the **Actions** panel.
4. Select a user to gain CodeSign Protect Administrator rights.

To create a code signing flow:

1. Open the **Venafi Configuration Console**.
2. Under the **Venafi Code Signing** node, select **Custom Flows**.
3. Select **Add new Code Signing Flow** in the **Actions** panel.
4. Enter a name for the Code Signing Flow.
5. Select the newly created Code Signing Flow and add an approver through the **Actions** panel.

To create an environment template for the code signing project:

1. Open the **Venafi Configuration Console**.
2. Under the **Venafi Code Signing** node, select **Environment Templates**.
3. Select **Certificate** in the **Actions** panel under **Add Single Template**.
4. Enter a name for the Code Signing Environment Template.
5. In the **Properties** window that appears, enter the **Description**, **Certificate Container**, and **Signing Flow** within the **Settings** tab.
6. Open the **Certificate Authority** tab and search for the previously configured **CA Template**. Select **Add**.
7. Open the **Keys** tab and select which key sizes to allow.
8. Open the **Key Storage** and open the drop-down menu.
9. Select the previously created **HSM Connector**.
10. Enter any optional information in the remaining tabs.

To create a new code signing project:

1. Log in to Aperture: `https://[IP_address_of_Venafi_TLS_Protect_Datacenter]/Aperture/codesign`.
2. Select **Projects**.
3. Select **Create Project**.
4. Enter a **Project Name** and **Description**.
5. Select **Create**.

To create an environment for the project with a new HSM private key and certificate:

1. Select the **Environments** tab.
2. Select **Create**.
3. Enter the **Environment Name**.
4. For **Environment Type**, select **Certificate & Key**.
5. For **Environment Template**, select the previously created Environment Template.
6. Optionally enter a value for **Time Constraint** and **IP Restrictions**.
7. Select **Next**.
8. **Signing Flow** should list your code signing flow and **Key Storage Location** should list your HSM Connector.
9. For **Creation Type**, select **Create new key**.
10. For **Certificate Provider**, select a CA.
11. For **Key Algorithm**, select a key algorithm.
12. Enter any other necessary information for the certificate.
13. Select **Create Environment**.
14. Select **Submit for Approval** to generate a new certificate and private key once it is approved.

To create an environment for the project with an existing HSM private key and certificate:

1. Select the **Environments** tab.
2. Select **Create**.
3. Enter the **Environment Name**.
4. For **Environment Type**, select **Certificate & Key**.
5. For **Environment Template**, select the previously created Environment Template.
6. Optionally enter a value for **Time Constraint** and **IP Restrictions**.
7. Select **Next**.
8. **Signing Flow** should list your code signing flow and **Key Storage Location** should list your HSM Connector.

9. For **Creation Type**, select **Use Existing**.
10. Import an existing certificate or manually enter its details.
11. Select an existing **Private HSM Key** and **Public HSM Key**.
12. For **Certificate Provider**, select a CA.
13. For **Key Algorithm**, select a key algorithm.
14. Enter any other necessary information for the certificate.
15. Select **Create Environment**.
16. Select **Submit for Approval** to generate a new certificate and private key once it is approved.

To approve the project:

1. Log in to Aperture: `https://[IP_address_of_Venafi_TLS_Protect_Datacenter]/Aperture/codesign`.
2. Select **Approvals**.
3. Select **Pending Approvals**.
4. Select the request.
5. Select **Approve/Reject**.
6. Enter a **Comment** for the approval.
7. Select **Approve**.
8. If you selected the option to generate new keys, the keys are now created on the Entrust nShield HSM. To list it, open a command prompt and run the following command:

```
nfkminfo -l
```